Cryptanalysis of RSA with small prime difference

Benne de Weger*

June 12, 2001

Abstract

We show that choosing an RSA modulus with a small difference of its prime factors yields improvements on the small private exponent attacks of Wiener and Boneh-Durfee.

Keywords
Cryptanalysis, RSA, Fermat Factoring, Wiener Attack, Boneh-Durfee Attack

1 Introduction

Let n be the modulus of an RSA key pair, i.e. a product of two large primes p, q. Let $\Delta = |p-q|$ be the *prime difference* of n. We will assume that the bitsizes of the primes are equal, hence equal to half the bitsize of n, so that the prime difference is at most as large as $n^{1/2}$. We note that when the primes are generated randomly and independently, then with overwhelming probability the prime difference will indeed be of the size of $n^{1/2}$. So in practice one can easily avoid small prime differences.

It is common knowledge amongst cryptologists that a too small prime difference makes RSA insecure. Namely, then Fermat's factoring technique can be applied. Standards sometimes mention this and consequently require a certain condition on Δ (e.g. ANSI X9.31 Sections 4.1.2 and C.3, see [ANSI], requiring that the two primes differ in the first 100 bits). On this matter the more popular applied cryptography handbooks however are inadequate (such as [MvOV, Note 8.8(ii)]) or even ignorant (such as [Sc, Section 19.3]), while these books (the first one more clear than the last one) do warn against the much more sophisticated attacks suitable for extremely large prime differences, such as elliptic curve factoring.

When $\Delta < n^{1/4}$ (in fact we mean $\Delta < cn^{1/4}$ for a c that is constant compared to n, but now and in the sequel we will ignore such constants), then the Fermat factoring technique gives an almost instantaneous result. As we did not find such an (almost trivial) quantitative result in the literature (however, see [Si]), we spend a few lines on it in Section 3.

Let e, d be the public and private exponents of the RSA key pair, which we assume to be reduced modulo $\phi(n)$ (the Euler totient function). Another well known attack on RSA, described

*Sportsingel 30, 2924 XN Krimpen aan den IJssel, The Netherlands, deweger@xs4all.nl

by Wiener [W] (see also [VvT]), uses continued fractions, and applies when the private exponent d is small. In particular, Wiener shows that RSA is insecure if $d < n^{1/4}$. This result has recently been improved by Boneh and Durfee [BD1], [BD2], who (heuristically but practically) use LLL to show that RSA is insecure whenever $d < n^{1-1/\sqrt{2}} = n^{0.292...}$. They conjecture that the right bound below which RSA is insecure is $d < n^{1/2}$ (apart from an epsilon).

It is the main theme of this note to show that these results of Wiener and Boneh and Durfee can easily be improved under the condition that the prime difference Δ is essentially smaller than its generic size of $n^{1/2}$. When the prime difference gets as small as $n^{1/4}$ (below which Fermat factoring already shows that RSA is insecure), our bounds for d below which RSA is insecure reach the conjectured $n^{1/2}$ for Wiener's attack, and even reach n for the Boneh and Durfee attack. Consequently, checking the size of the prime difference becomes more important if one wants to generate key pairs with small private exponents, e.g. to improve performance of private key operations.

More specifically, let $\Delta = n^{\beta}$ for $\beta \in \langle \frac{1}{4}, \frac{1}{2} \rangle$ (which is the proper range for β, as argued above), and let $d = n^{\delta}$. In Section 4 we show how Wiener's attack using continued fractions is effective whenever $\delta < \frac{3}{4} - \beta$ (in contrast to Wiener's $\delta < \frac{1}{4}$). We feel that our improvement to Wiener's attack will also go through for the extended Wiener attack as described by Verheul and Van Tilborg [VvT], but we did not investigate this in detail.

In Section 5 we show how the first result of Boneh and Durfee [BD1], that RSA is insecure when $\delta < \frac{7}{6} - \frac{1}{3}\sqrt{7}$, can be improved to $\delta < \frac{1}{6}(4\beta + 5) - \frac{1}{3}\sqrt{(4\beta + 5)(4\beta - 1)}$. Finally in Section 6 we show how the second result of Boneh and Durfee [BD2], that RSA is insecure when $\delta < 1 - \frac{1}{2}\sqrt{2}$, can be improved to $\delta < 1 - \sqrt{2\beta - \frac{1}{2}}$, but under the condition $\delta > 2 - 4\beta$. Note that these bounds equal the corresponding ones of Boneh and Durfee when $\beta = \frac{1}{2}$. The second bound is better, but holds only when $\beta > \frac{3}{8}$. The first bound approaches $\delta < 1$ as β approaches $\frac{1}{4}$.

Our main result, superseding all the others, is now given some status.

Observation

Let p, q be large primes of about the same size, and let $n = pq$. Let $\Delta = |p - q|$. Let e, d be integers > 1 and $< \phi(n)$, satisfying $ed \equiv 1 \pmod{\phi(n)}$. Put $\Delta = n^{\beta}$ and $d = n^{\delta}$.
Given only n and e, the factors p, q of n and the number d can be recovered efficiently whenever $2 - 4\beta < \delta < 1 - \sqrt{2\beta - \frac{1}{2}}$ or $\delta < \frac{1}{6}(4\beta + 5) - \frac{1}{3}\sqrt{(4\beta + 5)(4\beta - 1)}$.

The relevant regions for δ and β are visualized in Figure 1 below. Note that the ANSI X9.31 Standard ([ANSI]) requires $\beta > \frac{1}{2} - \frac{100}{\log_2 n}$ and $\delta > \frac{1}{2}$, which is strong enough to resist our attack, but for smaller bitsizes (such as 1024, see the big dot in Figure 1) leaves only a small margin.

Boneh and Durfee present heuristics to support their conjecture that the bound for δ below which RSA may be proved insecure is $\frac{1}{2}$. The same heuristic argument shows in our situation that the bound for δ, as a function of β, below which RSA may be proved insecure, is $\frac{3}{2} - 2\beta$. As this bound is an elegant function, is 1 at $\beta = \frac{1}{4}$, and is $\frac{1}{2}$ at $\beta = \frac{1}{2}$, we are tempted to conjecture it as the true bound (whatever that means).

For implementations of RSA key pair generation we recommend to build in a check for $\delta + 2\beta > \frac{7}{4}$, say. This is always much stronger than the ANSI X9.31 requirements, is very easy

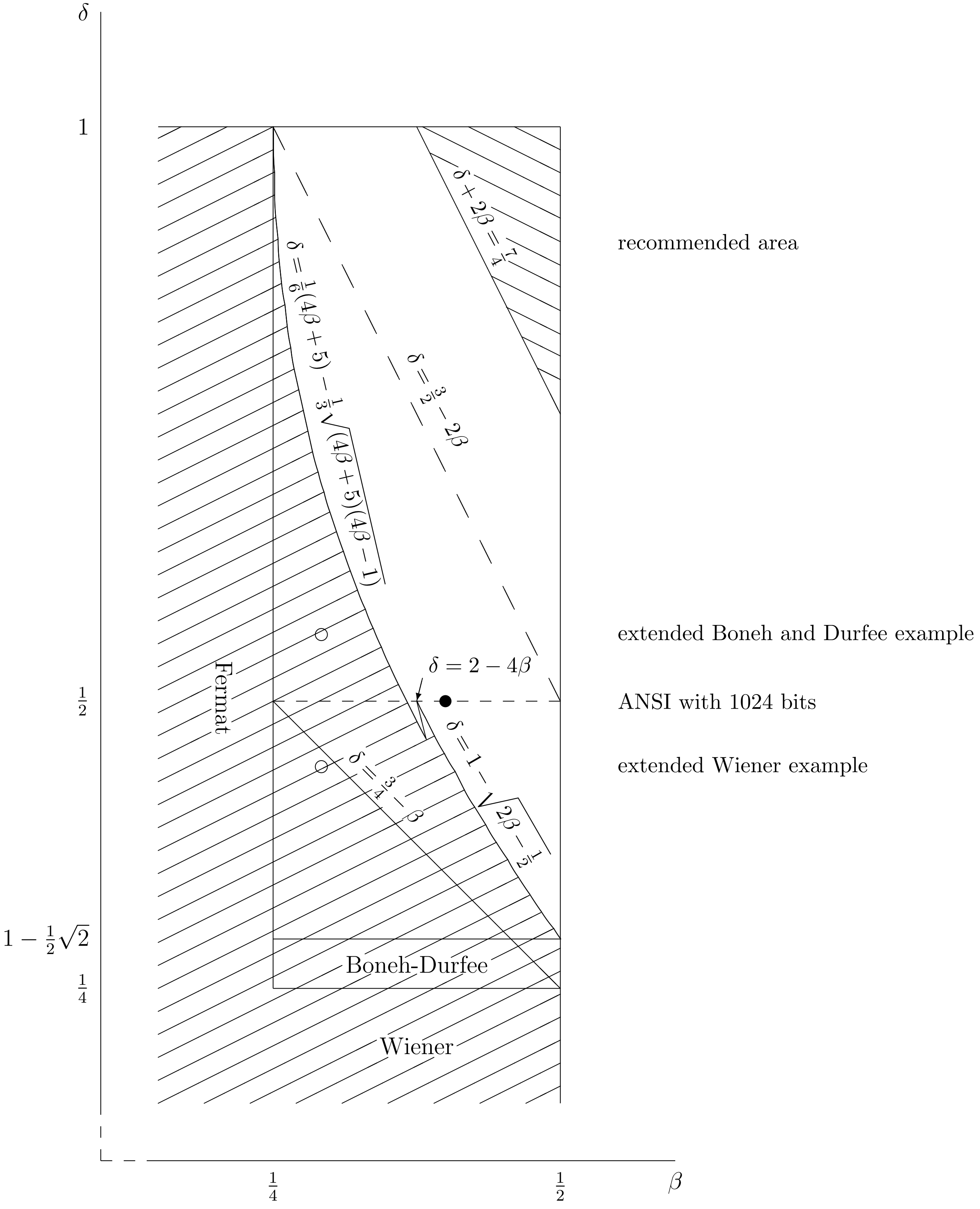

Figure 1: Regions for β and δ for which RSA is shown to be insecure.

to implement, and will only in extremely rare cases imply a performance loss because a key pair is to be rejected.

A suggestion for further work is to investigate whether the ideas of Coppersmith [C2] can be used to improve on the bounds of Boneh and Durfee [BD1], [BD2] in the situation where the high bits of p and q are known but not necessarily equal. Another suggestion is to investigate the possible improvements to our results when $e = n^\alpha$ for an α that is less than 1. Yet another suggestion is to investigate the effects on small private exponent attacks of p/q being close to some rational number (other than 1) with small numerator and denominator.

2 A lemma

A key role in all our arguments is played by the following simple lemma.

Lemma *If* $n = pq$ *and* $\Delta = p - q$ *then*

$$0 < p + q - 2n^{1/2} < \frac{\Delta^2}{4n^{1/2}}.$$

Proof. We have $\Delta^2 = (p+q)^2 - 4n = (p + q - 2n^{1/2})(p + q + 2n^{1/2})$, hence $p + q - 2n^{1/2} > 0$ and

$$p + q - 2n^{1/2} = \frac{\Delta^2}{p + q + 2n^{1/2}} < \frac{\Delta^2}{4n^{1/2}}.$$

$\square$

3 The Fermat factoring attack

In this section we show that when $\Delta < n^{1/4}$ (or a bit larger than that), Fermat's method of factoring n is very efficient. To be precise, we show that the complexity of Fermat factoring is $O(\frac{\Delta^2}{n^{1/2}})$. See also [Si].

Let $n = pq$ with p, q primes with $p > q$, and with difference $\Delta = p - q < n^{1/2}$. We assume that n is known, but that p and q are not. In Fermat factoring we try to find positive integers x, y (other than $x = n + 1, y = n - 1$), such that $4n = x^2 - y^2$. If we succeed, then we put $p = \frac{1}{2}(x + y)$ and $q = \frac{1}{2}(x - y)$, which are integers > 1 satisfying $pq = n$. Hence we have factored n. To find such x, y we simply try $x = \lceil 2n^{1/2} \rceil$, $\lceil 2n^{1/2} \rceil + 1$, $\lceil 2n^{1/2} \rceil + 2$, $\ldots$, until $x^2 - 4n$ is a square.

We study the number of values for x that have to be tried as a function of the prime difference Δ. As for each x only a small computation has to be done, this number is a good measure for the complexity of Fermat factoring. This number is $x + 1 - \lceil 2n^{1/2} \rceil$, which is approximately

$$x - 2n^{1/2} = p + q - 2n^{1/2} < \frac{\Delta^2}{4n^{1/2}},$$

by the Lemma from Section 2. It follows immediately that when $\Delta < cn^{1/4}$ then the number of tries is at most $\frac{1}{4}c^2$. When c is a (small) constant, this is independent of n (and not too large), and thus factoring n is trivial if, say, $\Delta < 1000n^{1/4}$.

4 Extending the Wiener attack

We now proceed to study the attack formulated by Wiener [W], which applies when the private exponent d is less than $n^{1/4}$, and we show that it can be extended from $\delta < \frac{1}{4}$ to $\delta < \frac{3}{4} - \beta$.

Wiener's attack works as follows. By the definition of e, d there exists a positive integer k such that $ed - k\phi(n) = 1$. We write this as

$$\frac{e}{\phi(n)} - \frac{k}{d} = \frac{1}{\phi(n)d}. \tag{1}$$

We know only n and e, and not $p, q, \phi(n), d$ or k. However, we do know that $\phi(n) = n+1-p-q$, and that p, q are of the size of $n^{1/2}$. So actually $\phi(n)$ is relatively close to n, and this is what Wiener exploits: (1) shows that the unknown fraction $\frac{k}{d}$ is a good approximation to $\frac{e}{\phi(n)}$, hence to $\frac{e}{n}$, which we do know. Thus we can use the continued fraction expansion of $\frac{e}{n}$ to compute good candidates for $\frac{k}{d}$ relatively fast.

To improve on this, we first notice that the error caused by replacing $\phi(n)$ by n is by far the dominating part of $\left|\frac{e}{n} - \frac{k}{d}\right|$. Then we notice that $n + 1 - 2n^{1/2}$ is a better approximation to $\phi(n)$ than n is. We have not found this information used anywhere in the literature. We find this somewhat surprising, but not too much, since in the general situation the upper bounds $|n - \phi(n)| < 3n^{1/2}$ and $|(n+1-2n^{1/2}) - \phi(n)| < n^{1/2}$ hold (approximately), and their difference is in the constant only. So the improvement seems not to be too important. However, for us it will be crucial to have the best available approximation to $\phi(n)$, as this is where we get the improvements from.

So by $n + 1 - \phi(n) = p + q$ and using the Lemma from Section 2 we find

$$0 < (n + 1 - 2n^{1/2}) - \phi(n) < \frac{\Delta^2}{4n^{1/2}}.$$

As a result we have from (1), and using $e < \phi(n)$, that

$$\begin{aligned} \left|\frac{e}{n+1-2n^{1/2}} - \frac{k}{d}\right| &< e\left|\frac{1}{n+1-2n^{1/2}} - \frac{1}{\phi(n)}\right| + \left|\frac{e}{\phi(n)} - \frac{k}{d}\right| \\ &< \phi(n)\frac{|(n+1-2n^{1/2}) - \phi(n)|}{(n+1-2n^{1/2})\phi(n)} + \frac{1}{\phi(n)d} \\ &< \frac{1}{\phi(n)}\left(\frac{\Delta^2}{4n^{1/2}} + \frac{1}{d}\right). \end{aligned}$$

Now we certainly may assume that $\phi(n) > \frac{3}{4}n$, and $n > 8d$. Hence, using $\Delta = n^{\beta}$ and $d = n^{\delta}$ we have

$$\left|\frac{e}{n+1-2n^{1/2}} - \frac{k}{d}\right| < \frac{1}{3}n^{2\beta-3/2} + \frac{4}{3nd} < \frac{1}{3}n^{2\beta-3/2} + \frac{1}{6n^{2\delta}},$$

and when we now take $2\beta - \frac{3}{2} < -2\delta$, i.e. $\delta < \frac{3}{4} - \beta$, then we obtain

$$\left|\frac{e}{n+1-2n^{1/2}} - \frac{k}{d}\right| < \frac{1}{2d^2}.$$

So if the condition $\delta < \frac{3}{4} - \beta$ holds, then $\frac{k}{d}$ is a convergent from the continued fraction expansion of $\frac{e}{n+1-2n^{1/2}}$, and we can find it efficiently. As is well known, knowledge of d makes it easy to factor n. This proves our claim. In the Appendix we present an example.

5 Extending the Boneh and Durfee attack, I

Boneh and Durfee [BD1], [BD2] describe an improvement of Wiener's attack that shows that RSA is insecure when $\delta < 1 - \frac{1}{2}\sqrt{2} = 0.292\ldots$, unconditionally. In [BD1] they give full details for the somewhat weaker result with the bound $\delta < \frac{7}{6} - \frac{1}{3}\sqrt{7} = 0.284\ldots$, which has a much simpler proof. Full details for their stronger attack are given in [BD2].

In this section we will show how to extend the weaker result of [BD1] to the case of small prime difference. In the next section we will do the same for the stronger result of [BD2]. Our claim in this section is that RSA is insecure whenever $\delta < \frac{1}{6}(4\beta+5) - \frac{1}{3}\sqrt{(4\beta+5)(4\beta-1)}$.

At the heart of the method of Boneh and Durfee is the idea to look at the equation $ed - k\phi(n) = 1$ modulo e, and to approximate $\phi(n)$ again by n (or $n+1$). Actually Boneh and Durfee take into consideration $\gcd(p-1, q-1)$, but for simplicity we will ignore that. So with $A = n+1$ as (known) approximation of $\phi(n)$ and $s = p+q$ as the (unknown) error of this approximation, they have an upper bound $|s| < e^{1/2}$ (note that e is approximately equal to n, again we freely ignore constants), and so they want to solve the *small inverse problem*

$$(-k)(A-s) \equiv 1 \pmod{e}, \quad |s| < e^{1/2}, |k| < e^{\delta}.$$

Then they use LLL to solve this problem. Note that we take the signs of k and s opposite from [BD1].

Heuristics easily show that the small inverse problem has a unique solution when $\delta < \frac{1}{2}$, which then can be used to break RSA. This leads Boneh and Durfee to the belief that this is the true bound for δ below which RSA is insecure.

As we have seen above in extending the Wiener attack, in the case of a small prime difference we have a better approximation to $\phi(n)$, namely $n+1-\lceil 2n^{1/2}\rceil$. So if we take $A = n+1-\lceil 2n^{1/2}\rceil$, then we can take $s = p+q-\lceil 2n^{1/2}\rceil$, for which by the Lemma of Section 2 we have the much better upper bound

$$|s| < \frac{\Delta^2}{4n^{1/2}} < e^{2\beta-1/2}$$

(ignoring constants and using $e \approx n$). Clearly this is trivial when $\beta \leq \frac{1}{4}$, but in that case we have the very efficient Fermat factoring method available. So we assume $\beta > \frac{1}{4}$. Then we have to solve the following small inverse problem:

$$(-k)(A-s) \equiv 1 \pmod{e}, \quad |s| < e^{2\beta-1/2}, |k| < e^{\delta}.$$

As the values of δ and β are not known, in practical applications upper bounds for them have to be guessed.

The same heuristics used by Boneh and Durfee show that this version of the small inverse problem has a unique solution when $\delta < \frac{3}{2} - 2\beta$. This is why we are tempted to believe that this is the true bound for δ below which RSA is insecure.

We now briefly describe the method of Boneh and Durfee to solve the small inverse problem. Let $f(x,y) = x(A+y) - 1$. Then we want to solve $f(x_0, y_0) \equiv 0 \pmod{e}$, $|x_0| < e^{\delta}$, $|y_0| < e^{2\beta-1/2}$. This is done, following an idea of Coppersmith [C1], by constructing polynomials that have (x_0, y_0) as root modulo e^m for some m, and then to make $\mathbb{Z}$-linear combinations of those polynomials, to find a few of them with small coefficients. When the coefficients are small enough, then a result of Howgrave-Graham [HG] shows that (x_0, y_0) actually is a root of $f(x, y)$ over $\mathbb{Z}$.

The polynomials to start from are the so-called x-shifts $g_{i,k}(x, y) = x^i f(x, y)^k e^{m-k}$ and y-shifts $h_{j,k}(x, y) = y^j f(x, y)^k e^{m-k}$, for $k = 0, \ldots, m$, $i = 0, \ldots, m - k$, $j = 0, \ldots, t$, for some t. With $X = e^{\delta}$, $Y = e^{2\beta-1/2}$ we now take the polynomials $g_{i,k}(xX, yY), h_{j,k}(xX, yY)$, and study the lattice spanned by their coefficient vectors. All lattice vectors now correspond to polynomials with (x_0, y_0) as root modulo e^m, and the theory of lattice basis reduction can be applied to yield both theoretical results about the existence of such polynomials with small coefficients, and practical results on how to efficiently find them. The result of [HG] now shows that this actually yields polynomials of which (x_0, y_0) is a root over $\mathbb{Z}$. When two such independent polynomials have been found, their resultant will most probably have a factor $x - x_0$ or $y - y_0$, which can easily be found.

All we now have to do to solve this variant of the small inverse problem is to work through the arguments of [BD1, Section 4] with for Y the new value $e^{2\beta-1/2}$. We assume that the reader has this paper available, as in the sequel we merely indicate the changes we make to its arguments, in order to avoid copying lots of details from Boneh and Durfee's papers.

In order to guarantee the existence of short enough vectors in the lattice, a condition on the determinant and the dimension has to be fulfilled. For the determinant of the lattice with only x-shifts, which has dimension $w = \frac{1}{2}m^2 + o(m^2)$, we find

$$\det{}_x = e^{(\frac{1}{4}+\frac{1}{3}\delta+\frac{1}{3}\beta+o(1))m^3},$$

so when we take no y-shifts at all, the condition $\det_x < e^{mw}$ to be fulfilled (up to a negligible constant) leads to the condition $\frac{1}{4} + \frac{1}{3}\delta + \frac{1}{3}\beta < \frac{1}{2}$. This is just $\delta < \frac{3}{4} - \beta$ as in Wiener's extended attack, presented in Section 4.

Including the y-shifts, reasoning as in [BD1, Section 4], we find for the contribution of the y-shifts to the determinant that

$$\det{}_y = e^{(\frac{1}{4}+\frac{1}{2}\delta+\beta)tm^2+(\beta-\frac{1}{4})t^2m+o(tm^2)}.$$

The condition $\det_x \det_y < e^{mw}$, with the dimension $w = \frac{1}{2}m^2 + tm + o(m^2)$, now leads to the condition

$$\left(-\frac{1}{4} + \frac{1}{3}\delta + \frac{1}{3}\beta\right) m^2 + \left(-\frac{3}{4} + \frac{1}{2}\delta + \beta\right) tm + \left(\beta - \frac{1}{4}\right) t^2 < 0.$$

The left hand side is minimal for $t = \frac{\frac{3}{4}-\frac{1}{2}\delta-\beta}{2\beta-\frac{1}{2}}m$, and substituting this, we find as condition (after clearing $4\beta - 1$ as denominator, which is positive)

$$16\beta^2 + 8\beta - 15 + (16\beta + 20)\delta - 12\delta^2 < 0.$$

This is equivalent to $\delta < \frac{1}{6}(4\beta + 5) - \frac{1}{3}\sqrt{(4\beta + 5)(4\beta - 1)}$, and thus we have proved our claim.

Note that for $\beta = \frac{1}{2}$ we recover Boneh and Durfee's result $\delta < \frac{7}{6} - \frac{1}{3}\sqrt{7}$, which should not come as a surprise. For $\beta \downarrow \frac{1}{4}$ we find that our condition approaches $\delta < 1$, which clearly is best possible.

6 Extending the Boneh and Durfee attack, II

In [BD2, Section B.3], Boneh and Durfee describe how they improved their result $\delta < \frac{7}{6} - \frac{1}{3}\sqrt{7}$ to $\delta < 1 - \frac{1}{2}\sqrt{2}$. We will now follow their arguments with, as in the previous section, $Y = e^{2\beta - 1/2}$ instead of $Y = e^{1/2}$, and again we only indicate changes to the arguments of [BD2]. Our aim is to show that RSA is insecure whenever $2 - 4\beta < \delta < 1 - \sqrt{2\beta - \frac{1}{2}}$.

Lemma B.5 from [BD2] can be improved to M_y being geometrically progressive with the obvious parameter choice $(m^{2m}, e, m, \delta + 2\beta - \frac{1}{2}, 2\beta - \frac{3}{2}, -1, 1, b)$ for some b. Here conditions (i), (ii) and (iii) of Definition B.1 are easily checked, but condition (iv) causes some trouble. Namely, b should satisfy $b(\delta + 2\beta - \frac{1}{2}) - 1 \geq 0$ and $b(2\beta - \frac{3}{2}) + 1 \geq 0$, and these conditions are contradictory when $\delta < 2 - 4\beta$. So we must assume $\delta > 2 - 4\beta$, and then we can take $b = \frac{2}{3 - 4\beta}$.

The optimal choice for t is $t = \frac{\frac{3}{2} - \delta - 2\beta}{2\beta - \frac{1}{2}} m$. We have

$$M_y(k, \ell, k, \ell) = e^{m + (\delta + 2\beta - 3/2)k + (2\beta - 1/2)\ell},$$

hence by our choice for t we have that $(k, \ell) \in S$ if and only if $\ell \leq \frac{\frac{3}{2} - \delta - 2\beta}{2\beta - \frac{1}{2}} k$. It follows that

$$w' = |S| = \left(\frac{\frac{3}{2} - \delta - 2\beta}{4\beta - 1} + o(1) \right) m^2,$$

and thus

$$w = \left(\frac{1}{2} + o(1) \right) m^2 + w' = \left(\frac{1 - \delta}{4\beta - 1} + o(1) \right) m^2.$$

A direct but somewhat tedious computation, closely following [BD2, Section B.3], leads to

$$\det(L'_y) = e^{\left(\frac{1}{12} \frac{9 - 4(\delta + 2\beta)^2}{4\beta - 1} + o(1) \right) m^3}.$$

A final computation then shows that the condition $\det(L_1) = \det_x \det(L'_y) < e^{mw}$, with $\det_x$ as in the previous section, is equivalent to $\delta < 1 - \sqrt{2\beta - \frac{1}{2}}$, which proves our claim.

We note that for $\beta = \frac{1}{2}$ we recovered Boneh and Durfee's result $\delta < 1 - \frac{1}{2}\sqrt{2}$, as expected. Further, the upper bound $\delta < 1 - \sqrt{2\beta - \frac{1}{2}}$ and the lower bound $\delta > 2 - 4\beta$ are contradictory when $\beta \leq \frac{3}{8}$ (or, equivalently, $\delta \geq \frac{1}{2}$). The exact regions for δ and β covered by the bounds of this and the previous sections are shown in Figure 1.

References

[ANSI] "ANSI X9.31-1998, Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)", *American National Standards Institute*, 1998.

[BBBCO] C. Batut, K. Belabas, D. Bernardi, H. Cohen and M. Olivier, "User's Guide to Pari-GP", Laboratoire A2X, Université Bordeaux, 2000.

[BD1] Dan Boneh and Glenn Durfee, ”Cryptanalysis of RSA with Private Key d less than $N^{0.292}$”, *Advances in Cryptology – EUROCRYPT'99*, Lecture Notes in Computer Science 1592, Springer-Verlag, Berlin, 1999, pp. 1–11.

[BD2] Dan Boneh and Glenn Durfee, ”New results on the Cryptanalysis of Low Exponent RSA”, *IEEE Transactions on Information Theory*, **46** No. 4 [2000], pp. 1339–1349.

[C1] Don Coppersmith, ”Finding a Small Root of a Univariate Modular Equation”, *Advances in Cryptology – EUROCRYPT'96*, Lecture Notes in Computer Science 1070, Springer-Verlag, Berlin, 1996, pp. 155–165.

[C2] Don Coppersmith, ”Finding a Small Root of a Bivariate Integer Equation; Factoring with High Bits Known”, *Advances in Cryptology – EUROCRYPT'96*, Lecture Notes in Computer Science 1070, Springer-Verlag, Berlin, 1996, pp. 178–189.

[HG] N. Howgrave-Graham, ”Finding Small Roots of Univariate Modular Equations Revisited”, Proceedings of Cryptography and Coding, Lecture Notes in Computer Science 1355, Springer-Verlag, Berlin, 1997, pp. 131–142.

[MvOV] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, ”Handbook of Applied Cryptography” , CRC Press, Boca Raton, 1997.

[Sc] Bruce Schneier, ”Applied Cryptography”, 2nd edition, Wiley, New York, 1996.

[Si] Robert D. Silverman, ”Fast Generation of Random, Strong RSA Primes”, *CryptoBytes* **3** No. 1 [1997], 9–13.

[VvT] Eric R. Verheul and Henk C.A. van Tilborg, ”Cryptanalysis of 'less short' RSA secret exponents”, *Applicable Algebra in Engineering, Communication and Computing* **8** [1997], 425–435.

[W] M. Wiener, ”Cryptana1ysis of short RSA secret exponents”, *IEEE Transactions on Information Theory* **36** [1990], 553–558.

Appendix Examples

An example for the extended Wiener attack

As an example let us take for n the 201 digit number

$$\begin{aligned} n = 1\,00000\,00000\,00000\,00000\,00000\,00000\,00000\,00000\,00107\,67242 \backslash \\ 83535\,54480\,74805\,52394\,71435\,44456\,91504\,57929\,40521\,29531 \backslash \\ 31145\,92588\,49187\,63903\,86483\,43076\,03736\,97739\,12905\,05518 \backslash \\ 23109\,11765\,96502\,73528\,89266\,92223\,96247\,82220\,51558\,89979\ , \end{aligned}$$

and for e the 199 digit number

$$\begin{aligned} e = \ 3577\,28738\,31168\,83468\,50061\,72494\,91494\,67592\,77183\,21983 \backslash \\ 42055\,05185\,69067\,45276\,16806\,40387\,24497\,92548\,46438\,84258 \backslash \\ 58859\,31908\,14322\,25357\,44998\,46915\,22809\,19771\,84669\,56259 \backslash \\ 50405\,61478\,87159\,75354\,13286\,66146\,64695\,96872\,98105\,35189\ . \end{aligned}$$

The first 200 partial quotients of $\frac{e}{n}$ are

$$\begin{aligned}
&[0, 27, 1, 20, 1, 4, 5, 1, 15, 1, 1, 1, 2, 1, 3, 1, 1, 29, 1, 2, 1, 1, 2, 1, 1,\\
&2, 1, 2, 3, 2, 1, 3, 1, 2, 1, 1, 1, 5, 1, 2400, 7, 2, 1, 46, 1, 1, 3, 1, 1, 1,\\
&11, 1, 16, 54, 1, 1, 1, 1, 7, 1, 1, 10, 1, 1, 1, 7, 19, 9, 1, 10, 3, 1, 3, 1, 1,\\
&1, 1, 1, 1, 30, 1, 2, 1, 19, 5, 1, 2, 1, 1, 1, 1, 5, 1, 1, 1, 5, 1, 4, 25, 1,\\
&3, 1, 3, 1, 1, 7, 1, 14, 1, 5, 6, 8, 2, 4, 4, 5, 3, 2, 6, 1, 13, 2, 2, 1, 14,\\
&1, 4, 1, 9, 3, 8, 7, 2, 9, 6, 1, 1, 1, 1, 2, 1, 1, 3, 3, 1, 41, 2, 6, 6, 6,\\
&3, 2, 1, 2, 1, 230, 8, 12, 5, 1, 3, 1, 1, 99, 1, 4, 5, 2, 7, 5, 4, 1, 16, 1, 4,\\
&40, 1, 3, 4, 1, 4, 1, 2, 1, 1, 6, 1, 1, 4, 5, 4, 4, 3, 5, 2, 8, 1, 9, 1, 1, 10, \ldots],
\end{aligned}$$

and we see no extraordinarily large one, so Wiener's attack as such will not give a result here. More partial quotients are not useful, since the 200th convergent already has a denominator that is much larger than $n^{1/4}$.

The first 200 partial quotients of $\frac{e}{n+1-2n^{1/2}}$ are

$$\begin{aligned}
&[0, 27, 1, 20, 1, 4, 5, 1, 15, 1, 1, 1, 2, 1, 3, 1, 1, 29, 1, 2, 1, 1, 2, 1, 1,\\
&2, 1, 2, 3, 2, 1, 3, 1, 2, 1, 1, 1, 5, 1, 2400, 7, 2, 1, 46, 1, 1, 3, 1, 1, 1,\\
&11, 1, 16, 54, 1, 1, 1, 1, 7, 1, 1, 10, 1, 1, 1, 7, 19, 9, 1, 10, 3, 1, 3, 1, 1,\\
&1, 1, 1, 1, 30, 1, 2, 1, 19, 5, 1, 2, 1, 1, 1, 1, 5, 1, 1, 1, 5, 1, 4, 25, 1,\\
&3, 1, 3, 1, 1, 7, 1, 14, 2, 7, 1, 11, 4, 1, 3, 1, 1, 1, 3, 3, 8, 1, 4, 1, 2,\\
&2, 2, 2, 1, 1, 1, 1, 1, 5, 22, 1, 2, 4, 1, 22, 1, 4, 2, 1, 15, 1, 1, 10, 4, 66,\\
&6, 3, 3, 2, 2, 36, 1, 1, 1, 1, 48, 2, 2, 13, 1, 1, 1, 2, 1, 10, 2, 1, 1, 2, 5,\\
&1, 29, 1, 12, 1, 56, 11, 147867491, 1, 3, 4, 2, 1, 1, 1, 1, 6, 3, 1, 3, 1, 2, 1, 5, 1, \ldots].
\end{aligned}$$

Now we see a large partial quotient, namely the 183th. The 182th convergent thus is an extremely good approximation to $\frac{e}{n+1-2n^{1/2}}$, and is a good candidate for $\frac{k}{d}$. It is

$$\begin{aligned}
k = {}& 125\,47153\,83488\,39464\,72356\,53791\,25074\,48077\,45478 \ \backslash\\
& 97673\,89403\,81525\,94977\,41329\,89005\,11062\,90778\,92359 \ ,\\
d = {}& 3507\,44921\,81144\,35074\,49218\,11443\,50744\,92181\,14435 \ \backslash\\
& 07449\,21811\,44350\,74492\,18114\,43507\,44921\,81144\,00389\,^{*},
\end{aligned}$$

and indeed with these k and d it is easy to factor n, as we will leave for the reader to show as an exercise.

Note that in this example $\delta \approx 0.443 > \frac{1}{4}$, which explains why Wiener's attack fails, and that $\beta \approx 0.292 > \frac{1}{4}$, indicating that also the Fermat factoring method will be rather inefficient. But our attack succeeds, since δ is just a little less than $\frac{3}{4} - \beta$ (we did not know this in advance). In Figure 1 a circle is drawn at the position of (β, δ) for this example.

Note that the first 108 partial quotients of $\frac{e}{n+1-2n^{1/2}}$ coincide with those of $\frac{e}{n}$, and that the first 182 (up to the large one) coincide with those of $\frac{e}{\phi(n)}$ (known only with hindsight).

[*] The repeating numbers 3507449 and 2181144 happen to be the author's bank account numbers.

An example for the extended Boneh and Durfee Attack

Next we take as an example for n the same 201 digit number as used above, and for e we take this time the 200 digit number

$$\begin{aligned} e = {} & 57244\,79358\,36564\,84515\,29075\,96780\,01067\,19671\,24315\,73871 \backslash \\ & 79961\,08242\,48083\,79435\,38065\,30972\,17276\,77453\,82992\,30049 \backslash \\ & 88402\,98193\,36998\,83948\,13822\,94539\,77463\,46393\,37937\,81478 \backslash \\ & 01649\,75097\,88795\,93740\,99999\,17419\,29447\,85381\,95823\,58977\ . \end{aligned}$$

Now we have to decide on the parameters for applying the method of Boneh and Durfee. We do not know the true values of δ and β, but the algorithm requires as input values for X and Y, as well as for m (the highest power of e) and t (the number of y-shifts). So we have to experiment a bit. It appears that in our situation $X = e^{0.56}, Y = e^{0.085}, m = 3, t = 2$ gives good results, but we did not do extensive experiments to find out optimal parameters. The choices of X and Y suggest that we expect a result in the neighbourhood of $\delta = 0.56, \beta = 0.29$.

With these parameters and with $A = n+1-\lceil 2n^{1/2} \rceil$ we built the 18-dimensional lattice from the x- and y-shifts, and started looking for a reduced basis. As programming tool we used Pari v2.0.20beta, see [BBBCO]. This program knows about the concept of *partially reduced basis*, which is a type of reduced lattice basis that is reduced in a weaker sense than LLL-reduced, but can be computed very quickly. We found that these partially reduced bases can be used for the Boneh and Durfee attack quite well, so this implies a substantial speedup of their method.

In our case of an 18-dimensional lattice with parameters as set above, we reached on our Pentium 800Mhz PC a result in only 43 seconds. To check the speedup we also computed a reduced basis in the LLL sense, which took 6 hours.

From the result we took, as in [BD1], resultants of the polynomials corresponding to the first two partially reduced basis vectors, and tried to factor these resultants. The resultant with respect to x turned out to have the linear factor $y + 15\,36705\,61801\,37046$. This suggests that $s = p + q - \lceil 2n^{1/2} \rceil = 15\,36705\,61801\,37046$, from which a candidate for $p + q$ is easily found. This indeed leads to the factorisation of n, as we leave to the reader to show.

Alternatively we could have used the resultant with respect to y, which turned out to have the linear factor

$$\begin{aligned} x+ \quad & \quad 20\,07832\,06496\,11816\,64118\,20947\,08544\,41560\,58908\,62520\,47042 \backslash \\ & 27985\,53951\,42154\,41920\,75567\,76391\,98360\,14586\,54592\,06249\,69194\,89182\ . \end{aligned}$$

This suggests that this polynomial is $x+k$ (which it indeed turns out to be), and from knowledge of k we easily can solve the problem again.

As a check for the reader we give d:

$$\begin{aligned} d = \quad & \quad 35\,07449\,21811\,44350\,74492\,18114\,43507\,44921\,81144\,35074\,49218\ \backslash \\ & 11443\,50744\,92181\,14435\,07449\,21811\,44350\,74492\,18114\,43507\,44921\,81393\,^{\dagger}. \end{aligned}$$

Note that in this example $\delta \approx 0.558 > \frac{1}{2}$, which explains why the Boneh and Durfee attack (as any other attack based only on δ, with the heuristic bound $\delta < \frac{1}{2}$) would probably fail in this case, and that $\beta \approx 0.292 > \frac{1}{4}$, so that $\delta + \beta > \frac{3}{4}$, indicating that also the extended Wiener attack will fail. In Figure 1 a circle is drawn at the position of (β, δ) for this example.

[†] Again featuring the author's bank account numbers.