Cryptanalysis of RSA with Private Key d Less than $N^{0.292}$

Dan Boneh* and Glenn Durfee**

Computer Science Department, Stanford University, Stanford, CA 94305-9045
{dabo,gdurf}@cs.stanford.edu

Abstract. We show that if the private exponent d used in the RSA public-key cryptosystem is less than $N^{0.292}$ then the system is insecure. This is the first improvement over an old result of Wiener showing that when $d < N^{0.25}$ the RSA system is insecure. We hope our approach can be used to eventually improve the bound to $d < N^{0.5}$.

1 Introduction

To provide fast RSA signature generation one is tempted to use a small private exponent d. Unfortunately, Wiener [10] showed over ten years ago that if one uses $d < N^{0.25}$ then the RSA system can be broken. Since then there have been no improvements to this bound. Verheul and Tilborg [9] showed that as long as $d < N^{0.5}$ it is possible to expose d in less time than an exhaustive search; however, their algorithm requires exponential time as soon as $d > N^{0.25}$.

In this paper we give the first substantial improvement to Wiener's result. We show that as long as $d < N^{0.292}$ one can efficiently break the system. We hope our approach will eventually lead to what we believe is the correct bound, namely $d < N^{0.5}$. Our results are based on the seminal work of Coppersmith [2].

Wiener describes a number of clever techniques for avoiding his attack while still providing fast RSA signature generation. One such suggestion is to use a large value of e. Indeed, Wiener's attack provides no information as soon as $e > N^{1.5}$. In contrast, our approach is effective as long as $e < N^{1.875}$. Consequently, larger values of e must be used to defeat the attack. We discuss this variant in Section 5.

2 Overview of Our Approach

Recall that an RSA public key is a pair $\langle N, e\rangle$ where $N = pq$ is the product of two n-bit primes. For simplicity, we assume $\gcd(p-1, q-1) = 2$. The corresponding private key is a pair $\langle N, d\rangle$ where $e \cdot d \equiv 1 \bmod \frac{\phi(N)}{2}$ where $\phi(N) = N - p - q + 1$.

* Supported by DARPA.
** Supported by Certicom and an NSF Graduate Research Fellowship.

J. Stern (Ed.): EUROCRYPT'99, LNCS 1592, pp. 1–11, 1999.

Note that both e and d are less than $\phi(N)$. It follows that there exists an integer k such that

$$ed + k\left(\frac{N+1}{2} - \frac{p+q}{2}\right) = 1. \tag{1}$$

Writing $s = -\frac{p+q}{2}$ and $A = \frac{N+1}{2}$, we know:

$$k(A+s) \equiv 1 \pmod{e}.$$

Throughout the paper we write $e = N^\alpha$ for some α. Typically, e is of the same order of magnitude as N (e.g. $e > N/10$) and therefore α is very close to 1. As we shall see, when α is much smaller than 1 our results become even stronger.

Suppose the private exponent d satisfies $d < N^\delta$. Wiener's results show that when $\delta < 0.25$ the value of d can be efficiently found given e and N. Our goal is to show that the same holds for larger values of δ. By equation (1) we know that

$$|k| < \frac{2de}{\phi(N)} \leq 3de/N < 3e^{1+\frac{\delta-1}{\alpha}}.$$

Similarly, we know that

$$|s| < 2N^{0.5} = 2e^{1/2\alpha}.$$

To summarize, taking $\alpha \approx 1$ (which is the common case) and ignoring constants, we end up with the following problem: find integers k and s satisfying

$$k(A+s) \equiv 1 \pmod{e} \quad \text{where} \quad |s| < e^{0.5} \ \text{ and } \ |k| < e^\delta. \tag{2}$$

The problem can be viewed as follows: given an integer A, find an element "close" to A whose inverse modulo e is "small". We refer to this is the *small inverse problem*. Clearly, if for a given value of $\delta < 0.5$ one can efficiently list all the solutions to the small inverse problem, then RSA with private exponent smaller than N^δ is insecure (simply observe that given s modulo e one can factor N immediately, since $e > s$). Currently we can solve the small inverse problem whenever $\delta < 1 - \frac{1}{2}\sqrt{2} \approx 0.292$.

Remark 1. A simple heuristic argument shows that for any $\epsilon > 0$, if k is bounded by $e^{0.5-\epsilon}$ (i.e. $\delta < 0.5$) then the small inverse problem (equation (2)) is very likely to have a unique solution. The unique solution enables one to break RSA. Therefore, the problem encodes enough information to prove that RSA with $d < N^{0.5}$ is insecure. For $d > N^{0.5}$ we have that $k > N^{0.5}$ and the problem will no longer have a unique solution. Therefore, we believe this approach can be used to show that $d < N^{0.5}$ is insecure, but gives no results for $d > N^{0.5}$.

The next section gives a brief introduction to lattices over $\mathbb{Z}^n$. Our solution to the small inverse problem when α is close to 1 is given in Section 4. In Section 5 we give a solution for arbitrary α. Section 6 describes experimental results with the algorithm.

3 Preliminaries

Let $u_1, \ldots, u_w \in \mathbb{Z}^n$ be linearly independent vectors with $w \leq n$. A lattice L spanned by $\langle u_1, \ldots, u_w \rangle$ is the set of all integer linear combinations of $u_1, \ldots, u_w$. We say that the lattice is full rank if $w = n$. We state a few basic results about lattices and refer to [7] for an introduction.

Let L be a lattice spanned by $\langle u_1, \ldots, u_w \rangle$. We denote by $u_1^*, \ldots, u_w^*$ the vectors obtained by applying the Gram-Schmidt process to the vectors $u_1, \ldots, u_w$. We define the determinant of the lattice L as

$$\det(L) := \prod_{i=1}^{w} \|u_i^*\|.$$

If L is a full rank lattice then the determinant of L is equal to the determinant of the $w \times w$ matrix whose rows are the basis vectors $u_1, \ldots, u_w$.

Fact 1 (LLL). *Let L be a lattice spanned by $\langle u_1, \ldots, u_w \rangle$. Then the LLL algorithm, given $\langle u_1, \ldots, u_w \rangle$, will produce a new basis $\langle b_1, \ldots, b_w \rangle$ of L satisfying:*

1. $\|b_i^*\|^2 \leq 2\|b_{i+1}^*\|^2$ *for all* $1 \leq i < w$.
2. *For all i, if* $b_i = b_i^* + \sum_{j=1}^{i-1} \mu_j b_j^*$ *then* $|\mu_j| \leq \frac{1}{2}$ *for all j.*

We note that an LLL-reduced basis satisfies some stronger properties, but those are not relevant to our discussion.

Fact 2. *Let L be a lattice and $b_1, \ldots b_w$ be an LLL-reduced basis of L. Then*

$$\|b_1\| \leq 2^{w/2} \det(L)^{1/w}.$$

Proof. Since $b_1 = b_1^*$ the bound immediately follows from:

$$\det(L) = \prod_i \|b_i^*\| \geq \|b_1\|^w 2^{-w^2/2}.$$

□

In the spirit of a recent result due to Jutla [5] we provide a bound on the norm of other vectors in an LLL reduced basis. For a basis $\langle u_1, \ldots, u_w \rangle$ of a lattice L, define

$$u_{\min}^* := \min_i \|u_i^*\|.$$

Fact 3. *Let L be a lattice spanned by $\langle u_1, \ldots, u_w \rangle$ and let $\langle b_1, \ldots b_w \rangle$ be the result of applying LLL to the given basis. Suppose $u_{min}^* \geq 1$. Then*

$$\|b_2\| \leq 2^{\frac{w}{2}} \det(L)^{\frac{1}{w-1}}$$

Proof. It is well known that $u^*_{\min}$ is a lower bound on the length of the shortest vector in L. Consequently, $\|b_1\| \geq u^*_{\min}$. We obtain

$$\det(L) = \prod_i \|b_i^*\| \geq \|b_1^*\| \cdot \|b_2^*\|^{w-1} 2^{-(w-1)^2/2} \geq u^*_{\min} \cdot \|b_2^*\|^{w-1} 2^{-(w-1)^2/2}.$$

Hence,

$$\|b_2^*\| \;\leq\; 2^{\frac{w-1}{2}} \left[\frac{\det(L)}{u^*_{\min}}\right]^{\frac{1}{w-1}} \leq 2^{\frac{w-1}{2}} \det(L)^{\frac{1}{w-1}},$$

which leads to

$$\|b_2\|^2 \;\leq\; \|b_2^*\|^2 + \frac{1}{4}\|b_1\|^2 \;\leq\; 2^{w-1} \det(L)^{\frac{2}{w-1}} + 2^{w-2} \det(L)^{\frac{2}{w}} \leq 2^w \det(L)^{\frac{2}{w-1}}.$$

Note that $\det(L) \geq 1$ since $u^*_{\min} \geq 1$. The bound now follows. □

Similar bounds can be derived for other b_i's. For our purposes the bound on b_2 is sufficient.

4 Solving the Small Inverse Problem

In this section we focus on the case when e is of the same order of magnitude as N, i.e. if $e = N^\alpha$ then α is close to 1. To simplify the exposition, in this section we simply take $\alpha = 1$. In the next section we give the general solution for arbitrary α. When $\alpha = 1$ the small inverse problem is the following: given a polynomial $f(x, y) = x(A + y) - 1$, find (x_0, y_0) satisfying

$$f(x_0, y_0) \equiv 0 \pmod{e} \quad \text{where} \quad |x_0| < e^\delta \;\text{ and }\; |y_0| < e^{0.5}.$$

We show that the problem can be solved whenever $\delta < 1 - \frac{1}{2}\sqrt{2} \approx 0.292$. We begin by giving an algorithm that works when $\delta < \frac{7}{6} - \frac{1}{3}\sqrt{7} \approx 0.285$. Our solution is based on a powerful technique due to Coppersmith [2], as presented by Howgrave-Graham [4]. We note that for this particular polynomial our results beat the generic bound given by Coppersmith. For simplicity, let $X = e^\delta$ and $Y = e^{0.5}$.

Given a polynomial $h(x, y) = \sum_{i,j} a_{i,j} x^i y^j$, we define $\|h(x, y)\|^2 := \sum_{i,j} |a_{i,j}^2|$. The main tool we use is stated in the following fact.

Fact 4 (HG98). *Let $h(x, y) \in \mathbb{Z}[x, y]$ be a polynomial which is a sum of at most w monomials. Suppose that*

a. $h(x_0, y_0) = 0 \bmod e^m$ for some positive integer m where $|x_0| < X$ and $|y_0| < Y$, and
b. $\|h(xX, yY)\| < e^m/\sqrt{w}$.

Then $h(x_0, y_0) = 0$ holds over the integers.

Proof. Observe that

$$|h(x_0, y_0)| = \left|\sum a_{i,j} x_0^i y_0^j\right| = \left|\sum a_{i,j} X^i Y^j \left(\frac{x_0}{X}\right)^i \left(\frac{y_0}{Y}\right)^j\right| \leq$$
$$\sum \left|a_{i,j} X^i Y^j \left(\frac{x_0}{X}\right)^i \left(\frac{y_0}{Y}\right)^j\right| \leq \sum \left|a_{i,j} X^i Y^j\right| \leq$$
$$\sqrt{w}\|h(xX, yY)\| < e^m,$$

but since $h(x_0, y_0) \equiv 0$ modulo e^m we have that $h(x_0, y_0) = 0$. □

Fact 4 suggests that we should be looking for a polynomial with small norm that has (x_0, y_0) as a root modulo e^m. To do so, given a positive integer m we define the polynomials

$$g_{i,k}(x, y) := x^i f^k(x, y) e^{m-k} \quad \text{and} \quad h_{j,k}(x, y) := y^j f^k(x, y) e^{m-k}.$$

We refer to the $g_{i,k}$ polynomials as x-shifts and the $h_{j,k}$ polynomials as y-shifts. Observe that (x_0, y_0) is a root of all these polynomials modulo e^m for $k = 0, \ldots, m$. We are interested in finding a low-norm integer linear combination of the polynomials $g_{i,k}(xX, yY)$ and $h_{j,k}(xX, yY)$. To do so we form a lattice spanned by the corresponding coefficient vectors. Our goal is to build a lattice that has sufficiently small vectors and then use LLL to find them. By Fact 2 we must show that the lattice spanned by the polynomials has a sufficiently small determinant.

Given an integer m, we build a lattice spanned by the coefficient vectors of the polynomials for $k = 0, \ldots, m$. For each k we use $g_{i,k}(xX, yY)$ for $i = 0, \ldots, m - k$ and use $h_{j,k}(xX, yY)$ for $j = 0, \ldots, t$ for some parameter t that will be determined later. For example, when $m = 3$ and $t = 1$ the lattice is spanned by the rows of the matrix in Figure 1. Since the lattice is spanned by a lower triangular matrix, its determinant is only affected by entries on the diagonal, which we give explicitly. Each "block" of rows corresponds to a certain power of x. The last block is the result of the y-shifts. In the example in Figure 1, $t = 1$, so only linear shifts of y are given. As we shall see, the y-shifts are the main reason for our improved results.

We now turn to calculating the determinant of the above lattice. A routine calculation shows that the determinant of the submatrix corresponding to all x shifts (i.e. ignoring the y-shifts by taking $t = 0$) is

$$\det_x = e^{m(m+1)(m+2)/3} \cdot X^{m(m+1)(m+2)/3} \cdot Y^{m(m+1)(m+2)/6}.$$

For example, when $m = 3$ the determinant of the submatrix excluding the bottom block is $e^{20} X^{20} Y^{10}$. Plugging in $X = e^\delta$ and $Y = e^{0.5}$ we obtain

$$\det_x = e^{m(m+1)(m+2)(5+4\delta)/12} = e^{\frac{5+4\delta}{12} m^3 + o(m^3)}.$$

It is interesting to note that the dimension of the submatrix is $w = (m+1)(m+2)/2$, and so the wth root of the determinant is $D_x = e^{m(5+4\delta)/6}$. For us to be

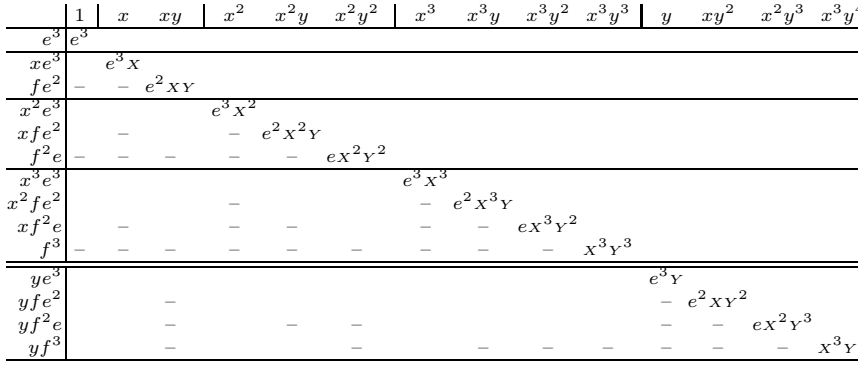

Fig. 1. The matrix spanned by $g_{i,k}$ and $h_{j,k}$ for $k = 0..3$, $i = 0..3 - k$, and $j = 0, 1$. The '–' symbols denote non-zero entries whose value we do not care about.

able to use Fact 4, we must have $D_x < e^m$, implying $(5 + 4\delta) < 6$. We obtain $\delta < 0.25$. This is exactly Wiener's result. Consequently, the lattice formed by taking all x-shifts cannot be used to improve on Wiener's result.

To improve on Wiener's result we include the y-shifts into the calculation. For a given value of m and t, the product of the elements on the diagonal of the submatrix corresponding to the y-shifts is:

$$\det_y = e^{tm(m+1)/2} \cdot X^{tm(m+1)/2} \cdot Y^{t(m+1)(m+t+1)/2}.$$

Plugging in the values of X and Y, we obtain:

$$\det_y = e^{tm(m+1)(1+\delta)/2+t(m+1)(m+t+1)/4} = e^{\frac{3+2\delta}{4}tm^2+\frac{mt^2}{4}+o(tm^2)}.$$

The determinant of the entire matrix is $\det(L) = \det_x \cdot \det_y$ and its dimension is $w = (m + 1)(m + 2)/2 + t(m + 1)$.

We intend to apply Fact 4 to the shortest vectors in the LLL-reduced basis of L. To do so, we must ensure that the norm of b_1 is less than $e^m/\sqrt{w}$. Combining this with Fact 2, we must solve for the largest value of δ satisfying

$$\det(L) < e^{mw}/\gamma,$$

where $\gamma = (w2^w)^{w/2}$. Since the dimension w is only a function of δ (but not of the public exponent e), γ is a fixed constant, negligible compared to e^{mw}. Manipulating the expressions for the determinant and the dimension to solve for δ requires tedious arithmetic. We provide the exact solution in the full version of this paper. Here, we carry out the computation ignoring low order terms. That is, we write

$$w = \frac{m^2}{2} + tm + o(m^2),$$
$$\det(L) = e^{\frac{5+4\delta}{12}m^3+\frac{3+2\delta}{4}tm^2+\frac{mt^2}{4}+o(m^3)}.$$

To satisfy $\det(L) < e^{mw}$ we must have

$$\frac{5+4\delta}{12}m^3 + \frac{3+2\delta}{4}tm^2 + \frac{mt^2}{4} < \frac{1}{2}m^3 + tm^2.$$

This leads to

$$m^2(-1+4\delta) - 3tm(1-2\delta) + 3t^2 < 0$$

For every m the left hand side is minimized at $t = \frac{m(1-2\delta)}{2}$. Plugging this value in leads to:

$$m^2\left[-1+4\delta - \frac{3}{2}(1-2\delta)^2 + \frac{3}{4}(1-2\delta)^2\right] < 0,$$

implying $-7 + 28\delta - 12\delta^2 < 0$. Hence,

$$\delta < \frac{7}{6} - \frac{1}{3}\sqrt{7} \approx 0.285.$$

Hence, for large enough m, whenever $d < N^{0.285-\epsilon}$ for any fixed $\epsilon > 0$ we can find a bivariate polynomial $g_1 \in \mathbb{Z}[x,y]$ such that $g_1(x_0, y_0) = 0$ over the integers. Unfortunately, this is not enough. To obtain another relation, we use Fact 3 to bound the norm of b_2. Observe that since the original basis for L is a triangular matrix, $u^*_{\min}$ is simply the smallest element on the diagonal. This turns out to be the element in the last row of the x-shifts, namely, $u^*_{\min} = X^m Y^m$, which is certainly greater than 1. Hence, Fact 3 applies. Combining Fact 4 and Fact 3 we see that b_2 will yield an additional polynomial g_2 satisfying $g_2(x_0, y_0) = 0$ if

$$\det(L) < e^{m(w-1)}/\gamma'$$

where $\gamma' = (w2^w)^{\frac{w-1}{2}}$. For large enough m, this inequality is guaranteed to hold, since the modifications only effect low order terms. Hence, we obtain another polynomial $g_2 \in \mathbb{Z}[x,y]$ linearly independent of g_1 such that $g_2(x_0, y_0) = 0$ over the integers. We can now attempt to solve for x_0 and y_0 by computing the resultant $h(x) = \mathrm{Res}_y(g_1, g_2)$. Then x_0 must be a root of $h(x)$. By trying all roots x_0 of $h(x)$ we find y_0 using $g_1(x_0, y)$.

Although the polynomials g_1, g_2 are linearly independent, they may not be algebraically independent; they might have a common factor. Indeed, we cannot guarantee that the resultant $h(x)$ is not identically zero. Consequently, we cannot claim our result as a theorem. At the moment it is a heuristic. Our experiments show it is a very good heuristic, as discussed in Section 6. The reason the algorithm works so well is that in our lattice, short vectors produced by LLL appear to behave as independent vectors.

Remark 2. The reader may be wondering why we construct the lattice L using x-shifts and y-shifts of f, but do not explicitly use mixed shifts of the form $x^i y^j f^k$. The reason is that all mixed shifts of f over the monomials used in L are already included in the lattice. That is, any polynomial $x^i y^j f^k e^{m-k}$ can be

expressed as an integer linear combination of x-shifts and y-shifts. To see this, observe that for any i, j, we have

$$x^i y^j = \sum_{u=0}^{i} \sum_{v=0}^{u} b_{u,v} x^{u-v} f^v + \sum_{u=1}^{j-i} \sum_{v=0}^{i} c_{u,v} y^u f^v$$

for some integer constants $b_{u,v}$ and $c_{u,v}$. Note that when $j \leq i$ the second summation is vacuous and hence zero. It now follows that

$$\begin{aligned} x^i y^j f^k e^{m-k} &= \sum_{u=0}^{i} \sum_{v=0}^{u} b_{u,v} e^v x^{u-v} f^{v+k} e^{m-v-k} + \sum_{u=1}^{j-i} \sum_{v=0}^{i} c_{u,v} e^v y^u f^{v+k} e^{m-v-k} \\ &= \sum_{u=0}^{i} \sum_{v=0}^{u} b_{u,v} e^v \cdot g_{u-v,v+k} + \sum_{u=1}^{j-i} \sum_{v=0}^{i} c_{u,v} e^v \cdot h_{u,v+k} \end{aligned}$$

Consequently, $x^i y^j f^k e^{m-k}$ is already included in the lattice.

4.1 Improved Determinant Bounds

The results of the last section show that the small inverse problem can be solved when $\delta < 0.285$. The bound is derived from the determinant of the lattice L. It turns out that the lattice L contains a sublattice with a smaller determinant. Working in this sublattice leads to improved results. The idea is to remove some of the rows that enlarge the determinant. We throw away the y-shifts corresponding to low powers of f. Namely, for all r and $i \geq (1 - 2\delta)r$, the polynomials $y^i f^r$ are not included in the lattice. Since these "damaging" y-shifts are taken out, more y-shifts can be included. More precisely, the largest y-shift can now be taken to be $t = m(1 - 2\delta)$ as opposed to $t = \frac{m(1-2\delta)}{2}$ used in the previous section.

The lattice constructed using these ideas is no longer full rank. In particular, the basis vectors no longer form a triangular matrix. As a result, the determinant must be bounded by other means. Nevertheless, an improvement on the bound on the determinant can be established, leading to the result that the small inverse problem can be solved for $\delta < 1 - \frac{1}{2}\sqrt{2} \approx 0.292$. We provide the details in the full version of this paper.

5 Cryptanalysis of Arbitrary e

In his paper, Wiener suggests using large values of e when the exponent d is small. This can be done by adding multiples of $\phi(N)$ to e before making it known as the public key. When $e > N^{1.5}$, Wiener's attack will fail even when d is small. We show that our attack applies even when larger values of e are used.

As described in Section 2, we solve the small inverse problem:

$$k(A + s) \equiv 1 \pmod{e} \quad \text{where} \quad |k| < 2e^{1+\frac{\delta-1}{\alpha}} \text{ and } |s| < 2e^{1/2\alpha},$$

for arbitrary values of α. We build the exact same lattice used in Section 4. Working through the calculations one sees that the determinant of the lattice in question is

$$\det_x(L) = e^{\frac{m^3}{3\alpha}(2\alpha+\delta-\frac{3}{4})+o(m^3)},$$
$$\det_y(L) = e^{\frac{tm^2}{2\alpha}(2\alpha+\delta-\frac{1}{2})+\frac{mt^2}{2}\frac{1}{2\alpha}+o(tm^2)}.$$

The dimension is as before. Therefore, to apply Fact 4 we must have

$$\frac{m^3}{3\alpha}(2\alpha+\delta-\frac{3}{4}) + \frac{tm^2}{2\alpha}(2\alpha+\delta-\frac{1}{2}) + \frac{mt^2}{2}\frac{1}{2\alpha} < \frac{m^3}{2} + tm^2,$$

which leads to

$$m^2(2\alpha+4\delta-3) - 3tm(1-2\delta) + 3t^2 < 0.$$

As before, the left hand side is minimized at $t_{\min} = \frac{1}{2}m(1-2\delta)$, which leads to

$$m^2[2\alpha+7\delta-\frac{15}{4}-3\delta^2] < 0,$$

and hence

$$\delta < \frac{7}{6} - \frac{1}{3}(1+6\alpha)^{1/2}.$$

Indeed, for $\alpha = 1$, we obtain the results of Section 4. The expression shows that when $\alpha < 1$ our attack becomes even stronger. For instance, if $e \approx N^{2/3}$ then RSA is insecure whenever $d < N^{\delta}$ for $\delta < \frac{7}{6} - \frac{\sqrt{5}}{3} \approx 0.422$. Note that if $e \approx N^{2/3}$ then d must satisfy $d > N^{1/3}$.

When $\alpha = \frac{15}{8}$ the bound implies that $\delta = 0$. Consequently, the attack becomes totally ineffective whenever $e > N^{1.875}$. This is an improvement over Wiener's bound, which become ineffective as soon as $e > N^{1.5}$.

6 Experiments

We ran some experiments to test our results when $d > N^{0.25}$. Our experiments were carried out using the LLL implementation available in Victor Shoup's NTL library. In all our experiments LLL produced two independent relations $g_1(x,y)$ and $g_2(x,y)$. In every case, the resultant $h(y) := \mathrm{Res}(g_1(x,y), g_2(x,y), x)$ with respect to x was a polynomial of the form $h(y) = (y+p+q)h_1(y)$, with $h_1(y)$ irredicible over $\mathbb{Z}$ (similarly for x). Hence, the unique solution (x_0, y_0) was correctly determined in every trial executed. Below we show the parameters of some attacks executed.

n	δ	m	t	lattice dimension	running time
1000 bits	0.265	5	3	39	45 minutes
3000 bits	0.265	5	3	39	5 hours
10000 bits	0.255	3	1	14	2 hours

These tests were performed under Solaris running on a 400MHz Intel Pentium processor. In each of these tests, d was chosen uniformly at random in the range $\left[\frac{3}{4}N^{\delta}, N^{\delta}\right]$ (thus guaranteeing the condition $d > N^{0.25}$). The last row of the table is especially interesting as it is an example in which our attack breaks RSA with a d that is 50 bits longer than Wiener's bound.

7 Conclusions and Open Problems

Our results show that Wiener's bound on low private exponent RSA is not tight. In particular, we were able to improve the bound from $d < N^{0.25}$ to $d < N^{0.285}$. Using an improved analysis of the determinant, we can show $d < N^{0.292}$. Our results also improve Wiener's attack when large values of e are used. We showed that our attack becomes ineffective only once $e > N^{1.875}$. In contrast, Wiener's attack became ineffective as soon as $e > N^{1.5}$.

Unfortunately, we cannot state our attack as a theorem since we cannot prove that it always succeeds. However, experiments that we carried out demonstrate its effectiveness. We were not able to find a single example where the attack fails. This is similar to the situation with many factoring algorithms, where one cannot prove that they work; instead one gives strong heuristic arguments that explain their running time. In our case, the heuristic "assumption" we make is that the two shortest vectors in an LLL reduced basis give rise to algebraically independent polynomials. Our experiments confirm this assumption. We note that a similar assumption is used in the work of Bleichenbacher [1] and Jutla [5].

Our work raises two natural open problems. The first is to make our attack rigorous. More importantly, our work is an application of Coppersmith's techniques to bivariate modular polynomials. It is becoming increasingly important to rigorously prove that these techniques can be applied to bivariate polynomials.

The second open problem is to improve our bounds. A bound of $d < N^{1-\frac{1}{\sqrt{2}}}$ cannot be the final answer. It is too unnatural. We believe the correct bound in $d < N^{1/2}$. We hope our approach eventually will lead to a proof of this stronger bound.

References

1. D. Bleichenbacher, "On the security of the KMOV public key cryptosystem", Proc. of Crypto '97, pp. 235–248.
2. D. Coppersmith, "Small solutions to polynomial equations, and low exponent RSA vulnerabilities", J. of Cryptology, Vol. 10, pp. 233–260, 1997.
3. J. Hastad, "Solving simultaneous modular equations of low degree", SIAM Journal of Computing, vol. 17, pp 336–341, 1988.
4. N. Howgrave-Graham, "Finding small roots of univariate modular equations revisited", Proc. of Cryptography and Coding, LNCS 1355, Springer-Verlag, 1997, pp. 131–142.
5. C. Jutla, "On finding small solutions of modular multivariate polynomial equations", Proc. of Eurocrypt '98, pp. 158–170.

6. A. Lenstra, H. Lenstra, and L. Lovasz. Factoring polynomial with rational coefficients. *Mathematiche Annalen*, 261:515–534, 1982.
7. L. Lovasz, "An algorithmic theory of numbers, graphs and convexity", SIAM lecture series, Vol. 50, 1986.
8. R. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, vol. 21, pp. 120–126, 1978.
9. E. Verheul, H. van Tilborg, "Cryptanalysis of less short RSA secret exponents", Applicable Algebra in Engineering, Communication and Computing, Springer-Verlag, vol. 8, pp. 425–435, 1997.
10. M. Wiener, "Cryptanalysis of short RSA secret exponents", IEEE Transactions on Info. Th., Vol. 36, No. 3, 1990, pp. 553–558.