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

Dan Boneh*
dabo@cs.stanford.edu

Glenn Durfee†
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 is less than $N^{0.25}$ the RSA system is insecure. We hope our approach can be used to eventually improve the bound to d less than $N^{0.5}$.

1 Introduction

To speed up RSA signature generation one is tempted to use a small private exponent d. Unfortunately, Wiener [14] 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 [13] 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. In particular, when $d < N^{0.292}$ an attacker can recover the private RSA key given the public key. 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 [3].

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 6.

2 Overview of Our Approach

Recall that an RSA public key is a pair of integers $\langle N, e\rangle$ 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 an integer d satisfying $e \cdot d \equiv 1 \bmod \frac{\phi(N)}{2}$ where $\phi(N) = N - p - q + 1$. Note that both e and d are typically less than $\phi(N)$. It follows that there exists an integer k such that

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

*Supported by NSF CCR-9732754.
†Supported by Certicom and an NSF Graduate Research Fellowship.
[0]An earlier version of this paper appeared in Eurocrypt '99 [2].

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, since both p and q are less than $2\sqrt{N}$ we know that

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

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

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

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 as 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 suggest that RSA with $d < N^{0.5}$ is insecure. For $d > N^{0.5}$ we have that $k > N^{0.5}$, so the small inverse 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 $\mathbb{Z}^n$. A first pass at a solution to the small inverse problem when α is close to 1 is given in Section 4. In Section 5, we improve this approach and prove the main result of the paper. Section 6 provides a solution for arbitrary α. In Section 7, we discuss a variant of our attack which works for *unbalanced* RSA moduli. These are moduli $N = pq$ where p is much larger than q. Finally, Section 8 describes experimental results with the attack 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 lattice basis reduction and refer to [9] for an introduction. Lattice basis reductions are frequently used in the cryptanalysis of public key systems [6].

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

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

where $\|.\|$ denotes the Euclidean norm on vectors. 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 3.1 (LLL) *Let L be a lattice spanned by $\langle u_1, \ldots, u_w \rangle$. The LLL algorithm, given $\langle u_1, \ldots, u_w \rangle$, runs in polynomial time and produces 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 3.2 *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:

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

In the spirit of a recent result due to Jutla [7] 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 3.3 *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. $\blacksquare$

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 $\delta < \frac{7}{6} - \frac{1}{3}\sqrt{7} \approx 0.284$. Our solution is based on a powerful technique due to Coppersmith [3], as presented by Howgrave-Graham [5]. 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. The fact shows that if a polynomial $h(x,y)$ has low norm then every small root of $h(x,y)$ modulo a big modulus is also a root of $h(x,y)$ over the integers.

Fact 4.1 (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

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

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

Fact 4.1 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 3.2 we must show that the lattice spanned by the polynomials has a sufficiently small determinant.

Given an integer m, we build a lattice L 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

	1	x	xy	x^2	x^2y	x^2y^2	x^3	x^3y	x^3y^2	x^3y^3	y	xy^2	x^2y^3	x^3y^4
e^3	e^3													
xe^3		e^3X												
fe^2	–	–	e^2XY											
x^2e^3				e^3X^2										
xfe^2		–		–	e^2X^2Y									
f^2e	–	–	–	–	–	eX^2Y^2								
x^3e^3							e^3X^3							
x^2fe^2				–			–	e^2X^3Y						
xf^2e		–		–	–		–	–	eX^3Y^2					
f^3	–	–	–	–	–	–	–	–	–	X^3Y^3				
ye^3											e^3Y			
yfe^2			–								–	e^2XY^2		
yf^2e			–		–	–					–	–	eX^2Y^3	
yf^3			–			–		–	–	–	–	–	–	X^3Y^4

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

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 lattice L. 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 w'th root of the determinant is $D_x = e^{m(5+4\delta)/6}$. For us to be able to use Fact 4.1, we must have $D_x < e^m$, implying $(5 + 4\delta) < 6$. We obtain $\delta < 0.25$. This is exactly Wiener's result. It turns out that any lattice formed by taking only the 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 4.1 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 3.2, 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 Appendix A. Here, we carry out the computation ignoring low order terms. That is, we write

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

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,

$$\delta < \frac{7}{6} - \frac{1}{3}\sqrt{7} \approx 0.284.$$

Hence, for large enough m, whenever $d < N^{0.284-\epsilon}$ 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 3.3 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 3.3 applies. Combining Fact 4.1 and Fact 3.3 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 y_0 by computing the resultant $h(y) = \mathrm{Res}_x(g_1, g_2)$. Then y_0 must be a root of $h(y)$. The roots of $h(y)$ are easily determined, and one such root will expose $y_0 = \frac{p+q}{2}$, allowing us to find the factorization of N.

Although the polynomials g_1, g_2 are linearly independent, they may not be algebraically independent; they might have a common factor. Indeed, in the general case 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 8. We could not find a single example where the algorithm fails. 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.

5 Improved Determinant Bounds

The results of the last section show that the small inverse problem can be solved when $\delta < 0.284$. The bound is derived from the determinant of the lattice L, which gives an upper bound on the lengths of the shortest vectors of the lattice. In this section, we improve the bounds on the lengths of the shortest vectors of L, and show that these improved bounds imply the attack is effective for all $d < N^{0.292}$.

We begin with a brief discussion of how we may improve the bounds on the shortest vectors. In the last section, we compute the determinant of a matrix M built from the coefficients vectors of shifts and powers of f. Since M is triangular, this is just the product of the entries on the diagonal, carefully balanced so that this product is less than e^{mw}. Once $\delta > 0.284$ the approach no longer works, as this product exceeds e^{mw} for every m. But if some of the larger, "damaging" terms of this product were removed, we might be able to afford greater values of δ. Intuitively, this suggests that we should "throw away" rows of M with large contributions to the diagonal. Unfortunately, the resulting lattice is not full rank, and computing its determinant is not so easy. What we will show is that a judicious choice of rows to eliminate results in lattice for which there is an improved bound on the determinant, leading to a successful attack for all $\delta < 0.292$. Specifically, we show that as long as $\delta < 0.292$, there is a rank $w' < w$ sublattice L' of L that satisfies the desired determinant bound of $e^{mw'}$. This results in better bounds on the length of the shortest vectors of L' (and hence of L). Most of this section is devoted to developing the necessary tools for bounding the determinant of non-full rank lattices. These results may be of independent interest.

We use the following approach. First, we introduce the notion of *geometrically progressive* matrices, and state the main theorem to be used to bound the determinant of a submatrix of any geometrically progressive matrix. A proof of this theorem is given in Appendix B. Second, we show that the portion of the matrix M developed in Section 4 corresponding to the y-shifts is geometrically progressive, yielding desirable bounds on the rectangular matrix formed from selected rows of M. Third, we review the new determinant computation and conclude that the attack outlined in Section 4 works for all $d < N^{0.292}$.

Geometrically Progressive Matrices

Recall the lattice L defined from the coefficients vectors of shifts and powers of the bivariate polynomial $f(x,y)$. Of particular interest is the inclusion of the y-shifts $h_{k,\ell}(xX,yY)$, which lead to a result improving on Wiener's bound. We begin by noting that there is a natural organization of these rows corresponding to y-shifts into "blocks" $h_{k,1},\ldots,h_{k,t}$ for $k=0,\ldots,m$, and that a similar organization is induced on the corresponding columns (that is, those columns that are zero in every row induced by an x-shift). To keep the results of this section general, we work with generic matrices in which the rows and columns have been divided into $a+1$ blocks of size b. Specifically, let a,b be positive integers and let M be an $(a+1)b\times(a+1)b$ matrix. We index the columns by pairs (i,j), with $i=0,\ldots,a$ and $j=1,\ldots,b$, so that the pair (i,j) corresponds to the $(bi+j)$th column of M. Similarly, we use the pair (k,ℓ) to index the $(bk+\ell)$th row of M, for $k=0,\ldots,a$ and $\ell=1,\ldots,b$. The entry in the (i,j)th column of the (k,ℓ)th row is denoted $M(i,j,k,\ell)$. Note that the diagonal entries of M are precisely those of the form $M(k,\ell,k,\ell)$.

Definition 5.1 *Let $C,D,c_0,c_1,c_2,c_3,c_4,\beta$ be real numbers with $C,\ D,\ \beta\geq 1$. A matrix M is said to be* geometrically progressive with parameters $(C,\ D,\ c_0,\ c_1,\ c_2,\ c_3,\ c_4,\ \beta)$ *if the following conditions hold for all $i,\ k=0,\ldots,a$ and $j,\ \ell=1,\ldots,b$:*

(i) $|M(i,j,k,\ell)|\leq C\cdot D^{c_0+c_1i+c_2j+c_3k+c_4\ell}$.

(ii) $M(k,\ell,k,\ell)=D^{c_0+c_1k+c_2\ell+c_3k+c_4\ell}$.

(iii) $M(i,j,k,\ell)=0$ *whenever $i>k$ or $j>\ell$.*

(iv) $\beta c_1+c_3\geq 0$ *and* $\beta c_2+c_4\geq 0$.

When the parameters $C,D,c_0,c_1,c_2,c_3,c_4,\beta$ are understood we say simply that M is geometrically progressive.

The following theorem bounds the determinant of a geometrically progressive matrix from which some rows are removed. A proof is given in Appendix B.

Theorem 5.1 *Let M be an $(a+1)b\times(a+1)b$ geometrically progressive matrix with parameters (C, D, c_0, c_1, c_2, c_3, c_4, β), and let B be a real number. Define*

$$S_B:=\{(k,\ell)\in\{0,\ldots,a\}\times\{1,\ldots,b\}\mid M(k,\ell,k,\ell)\leq B\},$$

and set $w:=|S_B|$. If L is the lattice defined by the rows $(k,\ell)\in S_B$ of M, then

$$\det(L)\leq((a+1)b)^{w/2}(1+C)^{w^2}\prod_{(k,\ell)\in S_B}M(k,\ell,k,\ell).$$

The basic idea is that when we remove rows with large entries on the diagonal, the resulting submatrix yields a sublattice with a determinant close to what is expected, to within a certain multiplicative error.

A Geometrically Progressive Submatrix

Recall the procedure outlined in Section 4 for creating the lattice L. We define the polynomials

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

and form a lattice from the coefficients vectors of every $g_{i,k}(xX, yY)$ and $h_{\ell,k}(xX, yY)$, for $k = 0, \dots, m$, $i = 0, \dots, m-k$, and $\ell = 1, \dots, t$.

We denote by M_y the portion of the matrix M with rows corresponding to the y-shifts $h_{\ell,k}$ and columns corresponding to variables of the form $x^u y^v$, $v > u$. Specifically, M_y is the $(m+1)t \times (m+1)t$ lower-right-hand submatrix of the matrix M presented in Section 4. We make the following claim about the entries of M_y.

Lemma 5.2 *For all positive integers m, t, the matrix M_y is geometrically progressive with parameters $(m^{2m},\ e,\ m,\ \frac{1}{2}+\delta,\ -\frac{1}{2},\ -1,\ 1,\ 2)$.*

Proof For simplicity, we take $e = N^\alpha$ with $\alpha = 1$. Let (k, ℓ) be given with $k = 0, \dots, m$ and $\ell = 1, \dots, t$. The row (k, ℓ) of M_y corresponds to the y-shift $h_{\ell,k}(xX, yY)$. Observe

$$h_{\ell,k}(xX, yY) = e^{m-k} y^\ell Y^\ell f^k(xX, yY) = \sum_{u=0}^{k} \sum_{v=0}^{u} c_{u,v} x^u y^{v+\ell},$$

where

$$c_{u,v} = \binom{k}{u}\binom{u}{v}(-1)^{k-u} e^{m-k} A^{u-v} X^u Y^{v+\ell}.$$

The column (i, j) for $i = 0, \dots, m$ and $j = 1, \dots, t$ corresponds to the coefficient of $x^i y^{i+j}$ in $h_{\ell,k}(xX, yY)$, which by the above is

$$M_y(i, j, k, \ell) = c_{i,i+j-\ell} = \binom{k}{i}\binom{i}{i+j-\ell}(-1)^{k-i} e^{m-k} A^{\ell-j} X^i Y^{i+j}.$$

It is easy to see that the above quantity equals 0 whenever $i > k$ or $j > \ell$, satisfying condition **(iii)**. Writing $X = e^\delta$, $Y = e^{\frac{1}{2}}$ and knowing $A < e$, we see

$$|M_y(i, j, k, \ell)| \le \left|\binom{k}{i}\binom{i}{i+j-\ell}(-1)^{k-i} e^{m+(\frac{1}{2}+\delta)i-\frac{1}{2}j-k+\ell}\right| \le m^{2m} \cdot e^{m+(\frac{1}{2}+\delta)i-\frac{1}{2}j-k+\ell},$$

satisfying condition **(i)**. Furthermore, a routine calculation confirms

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

satisfying condition **(ii)**. Lastly, observe $2\cdot(\frac{1}{2}+\delta)+(-1) = 2\delta \ge 0$ and $2\cdot -\frac{1}{2}+1 \ge 0$, so condition **(iv)** is met. Hence, M_y is geometrically progressive with parameters $(m^{2m},\ e,\ m,\ \frac{1}{2}+\delta,\ -\frac{1}{2},\ -1,\ 1,\ 2)$. ■

Remark 3. When $\alpha < 1$ we find that M_y is geometrically progressive with parameters $(m^{2m},\ e,\ m,\ \frac{1}{2\alpha}+\frac{\delta}{\alpha},\ \frac{1}{2\alpha}-1,\ -1,\ 1,\ 2\alpha)$. For $\alpha > 1$, we have that M_y is geometrically progressive with parameters $((2m)^{2m},\ e,\ m,\ \frac{1}{2\alpha}+\frac{\delta}{\alpha},\ -\frac{1}{2\alpha},\ -1,\ \frac{1}{\alpha},\ 2\alpha)$. The proofs of these statements follow as above, with the slight modification in the latter case where we use $A < 2e^{1/\alpha}$ instead of $A < e$.

Bounding the Determinant of the New Lattice

We now have the tools necessary to find improved bounds on the short vectors of L. Namely, we now would like to show that for all $d < N^{0.292}$, LLL finds short vectors in M that give rise to polynomials $g_1(x, y)$ and $g_2(x, y)$ such that $g_1(x_0, y_0) = 0$ and $g_2(x_0, y_0) = 0$ holds over the integers.

We begin by setting the parameter $t := (1-2\delta)k$. Note that this means our lattice will include twice as many y-shifts as used in Section 4, which, as we shall see, is the reason for the improved results. Define M_1 as follows: Take every row $g_{i,k}$ of M corresponding to the x-shifts, and take only those rows $h_{\ell,k}$ of M whose entry on the diagonal is less than or equal to e^m. That is, we throw away those rows $h_{\ell,k}$ where the the last entry exceeds e^m. Clearly, the lattice L_1 described by M_1 is a sublattice of L, so short vectors in L_1 will be in L.

Since all x-shifts are present in M_1, we may perform Gaussian elimination to set the first $(m+1)(m+2)/2$ off-diagonal columns of every row to zero. Specifically, there is a unitary matrix A over $\mathbb{R}$ such that $M_2 := AM_1$ is a matrix of the following form:

	$1\ x\ xy\ \cdots\ x^m y^m$	$y\quad y^2\quad \cdots\quad y^t$	$\cdots$	$x^m y^{m+1}\quad \cdots\quad x^m y^{m+t}$
x-shifts	Λ	0		
selected y-shifts	0	M'_y		

where Λ is a diagonal matrix and M'_y consists of selected rows of M_y. Furthermore, since A is unitary, the determinant of the lattice L_2 described by M_2 is equal to $\det(L_1)$.

We would like to obtain a good bound on $\det(L_2)$. Since the x-shifts and selected y-shifts portions of the lattice L_2 are orthogonal, it is sufficient to bound the determinant of each separately. Let w' be the number of rows of M'_y, and let L'_y be the lattice induced by M'_y. The determinant of the lattice L_2 is $\det(L_2) = \det(\Delta) \cdot \det(L'_y)$, and its dimension is $w = (m+1)(m+2)/2 + w'$. We aim to show $\det(L_2) < e^{mw}/\gamma$ where $\gamma = (w2^w)^{w/2}$. As we shall see, the dimension w is only a function of δ (but not of e), so γ is only a fixed constant, negligible compared to e^{mw}.

We begin by computing w'. Let $S \subseteq \{0, \ldots, m\} \times \{1, \ldots, t\}$ be the subset of indices such that $M_y(k, \ell, k, \ell) \leq e^m$ for $(k, \ell) \in S$, so that $w' = |S|$. Since $(k, \ell) \in S$ only if

$$e^{m + (\delta - \frac{1}{2})k + \frac{1}{2}\ell} < e^m,$$

we know $\ell \leq (1-2\delta)k$. Since we have taken $t = (1-2\delta)m$, we know every every pair (k, ℓ) satisfies $\ell \leq (1-2\delta)k \leq t$, so $\ell \leq (1-2\delta)k$ if and only if $(k, \ell) \in S$. Thus

$$w' = |S| = \sum_{k=0}^{m} \lfloor (1-2\delta)k \rfloor \geq \sum_{k=0}^{m} [(1-2\delta)k - 1] = (\frac{1}{2} - \delta)m^2 + o(m^2),$$

implying

$$w = w' + (m+1)(m+2)/2 = (1-\delta)m^2 + o(m^2).$$

Now we bound $\det(L'_y)$. Since this lattice is defined by the rows $(k, \ell) \in S$ of M_y, by Theorem 5.1 we have

$$\begin{aligned}
\det(L'_y) &\leq [(m+1)(1-2\delta)m]^{w'/2} (1 + m^{2m})^{(w')^2} \prod_{(k,\ell)\in S} M_y(k, \ell, k, \ell) \\
&\leq [(m+1)(1-2\delta)m]^{w'/2} (1 + m^{2m})^{(w')^2} \prod_{k=0}^{m} \prod_{\ell=0}^{\lfloor (1-2\delta)k \rfloor} e^{m + (\delta - \frac{1}{2})k + \frac{1}{2}\ell} \\
&\leq [(m+1)(1-2\delta)m]^{w'/2} (1 + m^{2m})^{(w')^2} e^{(\frac{5}{12} - \frac{2\delta}{3} - \frac{\delta^2}{3})m^3 + o(m^3)}.
\end{aligned}$$

Note that $[(m+1)(1-2\delta)m]^{w'/2}(1+m^{2m})^{(w')^2}$ is a function of only δ (but not of e), and thus is negligible compared to e^{m^3}. Finally, recall from Section 4 that

$$\det(\Delta) = \det{}_x = e^{m(m+1)(m+2)/3} \cdot X^{m(m+1)(m+2)/3} \cdot Y^{m(m+1)(m+2)/6} = e^{(\frac{5}{12}+\frac{\delta}{3})m^3+o(m^3)}.$$

Thus, we need the bound

$$\det(L_1) = \det(\Delta)\det(L'_y) \le e^{(\frac{5}{12}+\frac{\delta}{3})m^3+(\frac{5}{12}-\frac{2\delta}{3}-\frac{\delta^2}{3})m^3+o(m^3)} < e^{mw} = e^{(1-\delta)m^3+o(m^3)},$$

which leads to

$$\left(-\frac{1}{6}+\frac{2\delta}{3}-\frac{\delta^2}{3}\right)m^3+o(m^3) < 0,$$

implying $2\delta^2-4\delta+1 \ge 0$. Hence, we need

$$\delta < 1-\frac{\sqrt{2}}{2} \approx 0.292.$$

Thus, when $\delta < 0.292$, for sufficiently large m we have $\det(L_1) \le \gamma' e^{mw}$, implying the norm λ_1 of the shortest vector of L_1 satisfies $\lambda_1 \le \gamma' e^m$. Then the b_1 found by LLL in L satisfies $b_1 \le \gamma\gamma' e^m$, where $\gamma\gamma'$ depends only on δ and is thus negligible compared to e^m. This vector b_1 yields a polynomial $g_1(x,y)$ such that $g_1(x_0,y_0)$ holds over the integers.

Let M_1^* be the result of applying the Gram-Schmidt orthogonalization process to M_1. It is easy to see that the length of a vector in the x-shifts portion of M_1^* is simply the corresponding entry on the diagonal of M_1, and the length of a vector in the y-shifts portion of M^* is bounded from below by the corresponding entry on the diagonal of M_1. So $u_{\min}$ is simply X^mY^m, which is certainly greater than 1. So as in Section 4, a similar bound on b_2 can be established, yielding two linearly independent relations $g_1(x_0,y_0)=0$ and $g_2(x_0,y_0)=0$ which hold over the integers.

6 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 $e > N^{1.5}$ is 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

$$\begin{aligned}\det{}_x(L) &= e^{\frac{m^3}{3\alpha}(2\alpha+\delta-\frac{3}{4})+o(m^3)},\\ \det{}_y(L) &= e^{\frac{tm^2}{2\alpha}(2\alpha+\delta-\frac{1}{2})+\frac{mt^2}{2}\frac{1}{2\alpha}+o(tm^2)}.\end{aligned}$$

The dimension is as before. Therefore, to apply Fact 4.1 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 attack, which becomes ineffective as soon as $e > N^{1.5}$.

7 Cryptanalysis of Unbalanced RSA

In this section we study the case when the difference between the primes p and q is large. Suppose $p < N^\beta$, and $p < q$ (and therefore $\beta \leq 1/2$). For simplicity, we again assume that $e = N^\alpha$ with $\alpha \approx 1$.

Unfortunately, we cannot follow the approach of Section 4 directly, for the following reason. In this case, the small inverse problem now becomes: given a polynomial $f(x, y) = x(A + y) - 1$, find (x_0, y_0) satisfying

$$f(x_0, y_0) \equiv 0 \pmod{e} \quad \text{where} \quad |x_0| < e^\delta \text{ and } |y_0| < e^{1-\beta}.$$

Since only a weaker bound of $e^{1-\beta}$ is known on the solution $y_0 = p + q$, using the previous approach requires a stronger bound on x_0, and therefore δ. In fact, a routine calculation shows that once $\beta < 1/4$, this approach produces no results even for δ close to zero.

Therefore, a modified approach is needed. Returning to the RSA equation, recall equation (1):

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

Writing $A = N + 1$, we know:

$$k(A - p - q) \equiv 2 \pmod{e}.$$

As before, we know the bound

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

we now have $|p| < N^\beta$ and $|q| < N^{1-\beta}$.

We now have an equation with *three* unknowns, k, p, q, the product of two of which is known. We may view this problem as follows: given a polynomial $f(x, y, z) = x(A + y + z) - 2$, find (x_0, y_0, z_0) satisfying:

$$f(x_0, y_0, z_0) \equiv 0 \pmod{e} \quad \text{where} \quad |x_0| < e^\delta, \; |y_0| < e^\beta, \; |z_0| < e^{1-\beta}, \text{ and } y_0 z_0 = N.$$

We now follow an approach similar to the one used in Section 4. It is easy to prove a variant of Fact 4.1 for three variables, and as before, we wish to find a polynomial with small norm that has (x_0, y_0, z_0) as a root. Given an integer m we define the polynomials

- $g_{i,k}(x,y,z) := x^i f^k(x,y,z)e^{m-k}$,
- $h_{j,k}(x,y,z) := y^j f^k(x,y,z)e^{m-k}$, and
- $h'_{\ell,k}(x,y,z) := z^\ell f^k(x,y,z)e^{m-k}$,

taking care to substitute N for all occurrences of the product yz. We refer to the $g_{i,k}$ as the x-shifts, the $h_{j,k}$ as the y-shifts, and the $h'_{\ell,k}$ as the z-shifts. We are interested in finding a low-norm integer combination of the polynomials $g_{i,k}(xX, yY, zZ)$, $h_{j,k}(xX, yY, zZ)$, and $h'_{\ell,k}(xX, yY, zZ)$, where $X = N^\delta$, $Y = N^\beta$, and $Z = N^{1-\beta}$ are bounds on the respective variables. Again, we build a lattice from the coefficients vectors of the polynomials for all $k = 0, \ldots, m$; we use $i = 0, \ldots, m-k$, $j = 0, \ldots, t$, and $\ell = 0, \ldots, u$, for some t and u to be optimized later. We use LLL to find short vectors in this lattice, giving rise to two polynomials $G_1(x,y,z)$ and $G_2(x,y,z)$ that share (x_0, y_0, z_0) as a root over the integers. Plugging in $z = N/y$, we reduce these to the bivariate equations $H_1(x,y)$ and $H_2(x,y)$ and take resultants to reveal $y_0 = p$.

One additional optimization can be made. We modify the polynomials above, instead using $y^c g_{i,k}(xX, yY, zZ)$, $y^c h_{j,k}(xX, yY, zZ)$, and $y^c h'_{\ell,k}(xX, yY, zZ)$, for some c which can also be optimized. We refer to this as the *overall* shift. Now in order to use Fact 4.1 we require the resulting short vector to be less than the weaker bound of $p^c e^m$. This technique is most useful when q is much larger than p, since it eliminates occurrences of the variable z.

The optimization problem for t, u, and c is straightforward but tedious. Once the optimal overall shift and the optimal number of y- and z-shifts for a given β are found, the determinant of the resulting lattice will be small enough to use Facts 3.2 and 4.1 provided δ is sufficiently small. Below is a listing of values of δ for which we can launch a successful attack. Here we assume $p < N^\beta$ and $d < N^\delta$.

β	δ
1/2	0.2847
1/3	0.3183
1/4	0.3647
1/6	0.4412
1/10	0.5391
1/50	0.7750
1/100	0.8387
1/1000	0.9483

In these experiments, we did not take into account the optimizations suggested in Section 5. Therefore, further improvements may be possible.

It is interesting that low private key attacks become more effective for more unbalanced RSA moduli. Unbalanced moduli are used in *RSA for paranoids* introduced by Shamir [11].

8 Experiments

We ran several dozen 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 package [12]. In all our experiments

LLL produced two independent relations $g_1(x, y)$ and $g_2(x, y)$. In every case, the resultant $h(y) := \mathrm{Res}_x(g_1(x, y), g_2(x, y))$ with respect to x was a polynomial of the form $h(y) = (y + p + q)h_1(y)$, with $h_1(y)$ irreducible 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	d	δ	m	t	rank of lattice	running time	Advantage over Wiener's attack
1000 bits	280 bits	0.280	7	3	45	14 hours	30 bits
2000 bits	550 bits	0.275	7	3	45	65 hours	50 bits
4000 bits	1060 bits	0.265	5	2	25	14 hours	60 bits
10000 bits	2550 bits	0.255	3	1	11	90 minutes	50 bits

These tests were performed under Solaris running on a 500MHz Intel Pentium III 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 second to last row of the table is especially interesting as it is an example in which our attack breaks RSA with a private key that is 60 bits larger than Wiener's bound.

9 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 firstly from $d < N^{0.25}$ to $d < N^{0.2847}$. Using an improved analysis of the determinant, we obtained $d < N^{0.292}$. 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 [7].

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 some 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 is $d < N^{1/2}$. We hope our approach eventually will lead to a proof of this stronger bound.

To conclude, we note that Wiener suggested a defense against the low private exponent attack based on the Chinese Remainder Theorem (CRT). When $N = pq$ the idea is to use a private key d such that both $d_p = d \bmod (p-1)$ and $d_q = d \bmod (q-1)$ are small. Such d speed up RSA signature generation since RSA signatures are often generated modulo p and q separately and then combined using the CRT. Since $d_p \neq d_q$ the value of d is likely to be large, namely close to $\phi(N)$. Consequently, our low exponent attack does not apply to such d. It is an open problem whether there is an efficient attack on such private keys. The best known attack runs in time $\min(\sqrt{d_p}, \sqrt{d_q})$.

References

[1] D. Bleichenbacher. On the security of the KMOV public key cryptosystem. In proceedings *Crypto '97*, Lecture Notes in Computer Science, vol. 1294, Springer-Verlag, pp. 235-248, 1997.

[2] D. Boneh and G. Durfee. Cryptanalysis of RSA with Private Key d Less Than $N^{0.292}$. In proceedings *Eurocrypt '99*, Lecture Notes in Computer Science, vol. 1592, Springer-Verlag, pp. 1-11, 1999.

[3] D. Coppersmith. Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *Journal of Cryptology*, vol. 10, pp. 233–260, 1997.

[4] J. Håstad. Solving simultaneous modular equations of low degree. *SIAM Journal on Computing*, vol. 17, no. 2, pp. 336–341, 1988.

[5] N. Howgrave-Graham. Finding small roots of univariate modular equations revisited. In proceedings *Cryptography and Coding*, Lecture Notes in Computer Science, vol. 1355, Springer-Verlag, pp. 131–142, 1997.

[6] A. Joux and J. Stern. Lattice reductions: a toolbox for the cryptanalyst. *Journal of Cryptology*, vol. 11, no. 3, pp. 161–185, 1998.

[7] C. Jutla. On finding small solutions of modular multivariate polynomial equations. In proceedings *Eurocrypt '98*, Lecture Notes in Computer Science, vol. 1403, Springer-Verlag, pp. 158–170, 1998.

[8] A. Lenstra, H. Lenstra, and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, vol. 261, pp. 515–534, 1982.

[9] L. Lovász. An algorithmic theory of numbers, graphs, and convexity. *SIAM CBMS-NSF Regional Conference Series in Applied Mathematics*, vol. 50, 1986.

[10] R. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[11] A. Shamir. RSA for Paranoids. *RSA Laboratories CryptoBytes*, vol. 1, no. 3, pp. 1–4, 1995.

[12] V. Shoup. Number Theory Library (NTL), `http://www.shoup.net/ntl/`.

[13] E. Verheul and H. van Tilborg. Cryptanalysis of less short RSA secret exponents. *Applicable Algebra in Engineering, Communication, and Computing*, vol. 8, pp. 425–435, 1997.

[14] M. Wiener. Cryptanalysis of short RSA secret exponents. *IEEE Transactions on Information Theory*, vol. 36, no. 3, pp. 553–558, 1990.

A Appendix A: Precise Calculation of the Determinant

We give the exact expressions evaluating to the determinant of the lattice described in Section 4. We know

$$\begin{aligned} \det_x &= e^{m(m+1)(m+2)(5+4\delta)/12} \\ \det_y &= e^{tm(m+1)(1+\delta)/2+t(m+1)(m+t+1)/4} \end{aligned}$$

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

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

$$m(m+1)(m+2)\frac{5+4\delta}{12} + tm(m+1)\frac{1+\delta}{2} + \frac{t(m+1)(m+t+1)}{4} < \frac{m(m+1)(m+2)}{2} + tm(m+1)$$

Which leads to

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

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

$$-(3+2m+7m^2) + \delta(28m^2+20m) - 12m^2\delta^2 < 0$$

implying

$$\delta < \frac{7}{6} - \frac{1}{3}\sqrt{7 + \frac{16}{m} + \frac{4}{m^2}} + \frac{5}{6m}$$

As was shown in Section 4, when m goes to infinity this values converges to

$$\delta < \frac{7}{6} - \frac{\sqrt{7}}{3} \approx 0.2847$$

For a particular value of $\delta < 0.2847$ we must take m to be at least

$$m > \frac{-1 + 10\delta + 2(-5 + 16\delta + 16\delta^2)^{1/2}}{7 - 28\delta + 12\delta^2}$$

For example, when $\delta = 0.27$ we must take $m \geq 10$ leading to a lattice of dimension 86.

B Appendix B: Proof of Theorem 5.1

This Appendix provides a proof of Theorem 5.1.

We use the following approach. First we introduce the notion of *diagonally dominant* matrices, and show that there is an easy bound on the determinant of any lattice formed from a subset of the rows of a diagonally dominant matrix M. We then show that for certain submatrices of geometrically progressive matrices there is a unitary transformation over $\mathbb{R}$ that puts the submatrix into a diagonally dominant form, giving the desired determinant bounds. We then verify that these bounds yield the conclusion of Theorem 5.1.

Let M be an $n \times n$ triangular matrix with rows $u_1, \ldots, u_n$. We write the jth component of u_i as $u_{i,j}$. We say that M is *diagonally dominant to within a factor C* when $|u_{i,j}| \leq C \cdot |u_{i,i}|$ for all $i, j = 1, \ldots, n$. When the factor C is understood, we say simply that M is *diagonally dominant.*

Let S be a subset of the row indices. We define $M|_S$ to be the $|S| \times n$ matrix whose rows are $u_i, i \in S$. We say that an arbitrary $w \times n$ matrix $\tilde{M}$ is diagonally dominant when there is a $S \subseteq \{1, \ldots, n\}$ and diagonally dominant matrix M such that $\tilde{M} = M|_S$ and $|S| = w$. We say that a lattice L is diagonally dominant when there is a basis $u_1, \ldots, u_w$ for L such that the matrix with rows $u_1, \ldots, u_w$ is diagonally dominant. Diagonally dominant lattices have determinants that are easy to bound, as shown in the following fact.

Fact B.1 *Let $w \le n$ be given and take $S \subseteq \{1, \dots, n\}$ with $|S| = w$. If L is a lattice spanned by the rows $u_i, i \in S$ of a diagonally dominant matrix M, then*

$$\det(L) \le n^{w/2} C^w \prod_{i \in S} |u_{i,i}|.$$

Proof Observe that since $\|u_i^*\| \le \|u_i\|$ we have:

$$\det(L) = \prod_{i \in S} \|u_i^*\| \le \prod_{i \in S} \|u_i\| \le \prod_{i \in S} \sqrt{n} C |u_{i,i}| = n^{w/2} C^w \prod_{i \in S} |u_{i,i}|. \quad \blacksquare$$

Now let M be an $(a+1)b \times (a+1)b$ geometrically progressive matrix. Observe that if for every row (k, ℓ) the bound $D^{c_0+c_1 i+c_2 j+c_3 k+c_4 \ell}$ for the column (i, j) is less than the bound $D^{c_0+c_1 k+c_2 \ell+c_3 k+c_4 \ell}$ for the entry on the diagonal, then by conditions **(i)** and **(ii)** on geometrically progressive matrices we have that M is diagonally dominant to within a factor C. The columns of interest are those in which this bound does not hold; to wit, we call a column index (i, j) *bad* when the following condition holds:

$$D^{c_0+c_1 i+c_2 j+c_3 k+c_4 \ell} > D^{c_0+c_1 k+c_2 \ell+c_3 k+c_4 \ell},$$

or equivalently, $c_1(k - i) + c_2(\ell - j) < 0$. It should be noted that the "badness" of a column is a statement about the *bound* on the entry in the column, which is a function of the *parameters* of the geometrically progressive matrix, not of the entry itself. Indeed, the actual entry $M(i, j, k, \ell)$ of a bad column (i, j) could be zero, leading us to the following observation.

Remark B1. Let M be a geometrically progressive matrix and S a subset of the rows. If $M(i, j, k, \ell) = 0$ for every bad column (i, j) of every row $(k, \ell) \in S$, then $M|_S$ is diagonally dominant to within a factor C. This is because for each (i, j) that is not bad in the row (k, ℓ), we have

$$M(i, j, k, \ell) \le C \cdot D^{c_0+c_1 i+c_2 j+c_3 k+c_4 \ell} \le C \cdot D^{c_0+c_1 k+c_2 \ell+c_3 k+c_4 \ell} = C \cdot M(k, \ell, k, \ell).$$

Remark B1 suggests that we should be looking for a submatrix $M|_S$ whose entries are zero in bad columns. Although this is unlikely for any submatrix $M|_S$ of the matrix M developed in Section 4, what we shall see is that there is a unitary transformation over $\mathbb{R}$ that eliminates entries at bad columns in rows of $M|_S$. Once the diagonal dominance of this transformed submatrix has been established, Fact B.1 can then be employed to bound the determinant of the corresponding lattice.

Our goal now is to show that special submatrices of geometrically progressive matrices can be put into a diagonally dominant form. Consider the following situation: suppose we take a subset S of the rows of a geometrically progressive matrix M and wish to bound the determinant of the lattice described by $M|_S$. We wish to guarantee that there are "enough" rows included in S so that we may eliminate all nonzero entries at bad columns in rows of $M|_S$. We prove this for certain natural subsets S in Lemma B.2. We then use this guarantee to show that such an elimination procedure will be successful; namely, we show that there is a unitary transformation U over $\mathbb{R}$ such that $U \cdot M|_S$ is diagonally dominant. This is shown in Lemma B.3, leading directly to a proof of Theorem 5.1.

Lemma B.2 *Let M be an $(a+1)b \times (a+1)b$ geometrically progressive matrix with parameters (C, D, c_0, c_1, c_2, c_3, c_4, β), let $B \in \mathbb{R}$ be a constant. Define*

$$S_B := \{(k, \ell) \in \{0, \dots, a\} \times \{1, \dots, b\} \mid M(k, \ell, k, \ell) \le B\}.$$

For all $(k, \ell) \in S_B$ and $i \le k, j \le \ell$, if column (i, j) is bad in row (k, ℓ) then $(i, j) \in S_B$.

Proof We begin by assuming that (i,j) is bad, so $D^{c_1(k-i)+c_2(\ell-j)} < 1$ and thus

$$D^{(\beta-1)c_1(k-i)+(\beta-1)c_2(\ell-j)} = \left(D^{c_1(k-i)+c_2(\ell-j)}\right)^{(\beta-1)} \leq 1. \tag{3}$$

Seeking contradiction, we now assume $(i,j) \notin S_B$, that is, $M(i,j,i,j) > B$. It follows that

$$D^{(c_1+c_3)i+(c_2+c_4)j} = M(i,j,i,j) > B \geq M(k,\ell,k,\ell) = D^{(c_1+c_3)k+(c_2+c_4)\ell}.$$

Hence

$$D^{(c_1+c_3)(k-i)+(c_2+c_4)(\ell-j)} < 1. \tag{4}$$

Combining equations (3) and (4) yields

$$D^{(\beta c_1+c_3)(k-i)+(\beta c_2+c_4)(\ell-j)} < 1. \tag{5}$$

Note that $i \leq k$ and $j \leq \ell$ by the hypotheses of the theorem, and we are guaranteed $\beta c_1 + c_3 \geq 0$ and $\beta c_2 + c_4 \geq 0$ since M is geometrically progressive. So $(\beta c_1 + c_3)(k-i) + (\beta c_2 + c_4)(\ell - j) \geq 0$. Furthermore, $D \geq 1$, so

$$D^{(\beta c_1+c_3)(k-i)+(\beta c_2+c_4)(\ell-j)} \geq D^0 = 1,$$

contradicting equation (5). Hence, $(i,j) \in S_B$ as desired. ■

Lemma B.3 *Let M be an $(a+1)b \times (a+1)b$ geometrically progressive matrix with parameters (C, D, c_0, c_1, c_2, c_3, c_4, β), let $B \in \mathbb{R}$ be a constant, define*

$$S_B := \{(k,\ell) \in \{0,\ldots,a\} \times \{1,\ldots,b\} \mid M(k,\ell,k,\ell) \leq B\},$$

and set $w := |S_B|$. There is a $w \times w$ unitary matrix U over $\mathbb{R}$ such that $U \cdot M|_{S_B}$ is diagonally dominant to within a factor $(1+C)^w$.

Proof We proceed by induction. There are w rows in the matrix $M|_{S_B}$, and we build matrices U_r such that the last r rows of $U_r \cdot M|_{S_B}$ are diagonally dominant[1] to within a factor $(1+C)^w$, and the first $w-r$ rows identical to those in $M|_{S_B}$. The U we seek is U_w.

Clearly, $U_0 = I$ trivially satisfies this condition. Now suppose we have a unitary matrix U_{r-1} over $\mathbb{R}$ such that the last $r-1$ rows of $U_{r-1} \cdot M|_{S_B}$ are diagonally dominant to within a factor $(1+C)^w$ and the first $w-r$ rows are identical to those of $M|_{S_B}$. We would like to find U_r that satisfies this condition for the last r rows, and we do this by finding a unitary matrix V over $\mathbb{R}$ such that $U_r := V \cdot U_{r-1}$ satisfies this condition. Roughly speaking, the purpose of V is to "clean up" row $(w-r+1)$ of $M|_{S_B}$; that is, it guarantees that $(1+C)^w$ times the last column of row $(w-r+1)$ dominates all other columns of row $(w-r+1)$ in $V \cdot U_{r-1} \cdot M|_{S_B}$.

Since $M|_{S_B}$ is formed from rows of M, we may choose a pair (k,ℓ) such that row $(w-r+1)$ of $M|_{S_B}$ is the (k,ℓ)th row of M. By Lemma B.2, for every bad column (i,j) satisfying $i \leq k$ and $j \leq \ell$, the corresponding row (i,j) is in S_B. So there are at most $w-1$ bad columns with nonzero entries in the row (clearly, (k,ℓ) is not bad.)

We build V in stages by constructing elementary row operations $V_1,\ldots,V_{w-1}$ and letting $V := V_{w-1} \cdot V_{w-2} \cdots V_1$. Each V_s sets another bad column (i_s,j_s) in the row to 0, so that the $(w-r+1)$th row of $V_s \cdots V_1 \cdot U_{r-1} \cdot M|_{S_B}$ has nonzero entries in at most $w-s-1$ bad columns. We show that each V_s increases every column of the row by at most a factor of $(1+C)$.

[1] To say that the last r rows of a $w \times n$ matrix $\tilde{M}$ are diagonally dominant means simply that $\tilde{M}|_{(w-r+1),\ldots,w}$ is diagonally dominant.

Define

$$v^{(s)} := (V_s \cdots V_1 \cdot U_{r-1} \cdot M|_{S_B})|_{\{w-r+1\}},$$

that is, $v^{(s)}$ is the $(w+r-1)$th row of $V_s \cdots V_1 \cdot U_{r-1} \cdot M|_{S_B}$. We denote the entry in the (i,j)th column of $v^{(s)}$ as $v^{(s)}(i,j)$. We maintain the following three invariants for $s = 1, \ldots, w-1$:

(i) $\left|v^{(s)}(i,j)\right| \leq (1+C)^s C \cdot D^{c_0+c_1 i+c_2 j+c_3 k+c_4 \ell}$ for all columns (i,j);

(ii) $i > k$ or $j > \ell$ implies $v^{(s)}(i,j) = 0$; and,

(iii) the number of bad columns with nonzero entries in $v^{(s)}$ is at most $w-s-1$.

These conditions are satisfied trivially for $s = 0$, since $v^{(0)}$ is identical to row (k,ℓ) of the geometrically progressive matrix M. Now suppose that every column (i,j) of $v^{(s-1)}$ satisfies these three conditions. If there are no nonzero entries of $v^{(s-1)}$ at bad columns, we are done, and may take $V_s, \ldots, V_{w-1} := I$. Otherwise, let (i_s, j_s) be the rightmost bad column such that $v^{(s-1)}(i_s,j_s) \neq 0$. Since $v^{(s-1)}(i_s,j_s) \neq 0$, we know by the inductive hypothesis that $i_s \leq k$ and $j_s \leq \ell$. Since (i_s,j_s) is also bad, we know that $(i_s,j_s) \in S_B$. So we may pick a t such that row (i_s,j_s) of M is row t of $M|_{S_B}$. Define V_s to be the elementary row operation that subtracts $\frac{v^{(s-1)}(i_s,j_s)}{M(i_s,j_s,i_s,j_s)}$ times row t from row $(w-r+1)$. Observe for every column (i,j),

$$\begin{aligned}
\left|v^{(s)}(i,j)\right| &\leq \left|v^{(s-1)}(i,j)\right| + \left|\frac{v^{(s-1)}(i_s,j_s)}{M(i_s,j_s,i_s,j_s)} \cdot M(i,j,i_s,j_s)\right| \\
&\leq (1+C)^{s-1} C \cdot D^{c_0+c_1 i+c_2 j+c_3 k+c_4 \ell} \\
&\quad + \frac{(1+C)^{s-1} C \cdot D^{c_0+c_1 i_s+c_2 j_s+c_3 k+c_4 \ell}}{D^{c_0+c_1 i_s+c_2 j_s+c_3 i_s+c_4 j_s}} \cdot C \cdot D^{c_0+c_1 i+c_2 j+c_3 i_s+c_4 j_s \ell} \\
&= (1+C)^s C \cdot D^{c_0+c_1 i+c_2 j+c_3 k+c_4 \ell}.
\end{aligned}$$

So condition **(i)** is met.

Now let (i,j) be given with either $i > k$ or $j > \ell$. Since $v^{(s-1)}(i_s,j_s) \neq 0$, we know by condition **(ii)** of the inductive hypothesis that $i_s \leq k$ and $j_s \leq \ell$. So either $i > k \geq i_s$ or $j > \ell \geq j_s$, implying $M(i,j,i_s,j_s) = 0$. Thus

$$v^{(s)}(i,j) = v^{(s-1)}i,j - \frac{v^{(s-1)}(i_s,j_s)}{M(i_s,j_s,i_s,j_s)} \cdot M(i,j,i_s,j_s) = 0 - 0 = 0,$$

satisfying condition **(ii)**.

We now claim that the number of bad columns with nonzero entries in $v^{(s)}$ is at most $w-s-1$. Clearly, $v^{(s)}(i_s,j_s) = 0$, and columns to the right of (i_s,j_s) are unchanged from $v^{(s-1)}$. Since (i_s,j_s) was chosen to be the rightmost nonzero bad column of $v^{(s-1)}$, this implies that no nonzero column in $v^{(s)}$ to the right of (i_s,j_s) is bad. But since this is the sth elimination step, there are at least $s-1$ bad columns (i,j) to the right of (i_s,j_s) satisfying $i \leq k$ and $j \leq \ell$. Thus, the number of bad columns with nonzero entries in $v^{(s)}$ is at most $w-s-1$, satisfying condition **(iii)**.

Thus, $v^{(w-1)}$ has a zero in every bad column, so

$$v^{(w-1)}(i,j) \leq (1+C)^{w-1} C \cdot D^{c_1 i+c_2 j+c_3 k+c_4 \ell} \leq (1+C)^w \cdot M(k,\ell,k,\ell)$$

for all columns (i,j). Setting $V := V_{w-1} \cdots V_1$ and $U_r := V \cdot U_{r-1}$, we have that the last r rows of $U_r \cdot M|_{S_B}$ are diagonally dominant to within a factor $(1+C)^w$. Finally, taking $U := U_w$ completes the result. ■

We are now ready to complete the proof of Theorem 5.1.

Proof of Theorem 5.1 By Lemma B.3 we have a $w \times w$ unitary matrix U over $\mathbb{R}$ such that $U \cdot M|_{S_B}$ is diagonally dominant to within a factor $(1+C)^w$. Since U is unitary over $\mathbb{R}$, the lattice L' induced by the rows of $U \cdot M|_{S_B}$ has the same determinant as the lattice L induced by the rows of $M|_{S_B}$, so by Fact B.1 yielding the desired bound

$$\det(L) = \det(L') \leq ((a+1)b)^{w/2}(1+C)^{w^2} \prod_{(k,\ell)\in S_B} M(k,\ell,k,\ell).$$ ■