Low Secret Exponent RSA Revisited

J. Blömer, A. May

Department of Mathematics and Computer Science
University of Paderborn
33095 Paderborn, Germany
{*bloemer,alexx*}*@uni-paderborn.de*

Abstract. We present a lattice attack on low exponent RSA with short secret exponent $d = N^\delta$ for every $\delta < 0.29$. The attack is a variation of an approach by Boneh and Durfee [4] based on lattice reduction techniques and Coppersmith's method for finding small roots of modular polynomial equations. Although our results are slightly worse than the results of Boneh and Durfee they have several interesting features. We partially analyze the structure of the lattices we are using. For most $\delta < 0.29$ our method requires lattices of smaller dimension than the approach by Boneh and Durfee. Hence, we get a more practical attack on low exponent RSA. We demonstrate this by experiments, where $\delta > 0.265$.
Our method as well as the method by Boneh and Durfee is a heuristic, since the method is based on Coppersmith's approach for bivariate polynomials. Coppersmith [6] pointed out that this heuristic must fail in some cases. We argue in this paper, that a (practically not interesting) variant of the Boneh/Durfee attack proposed in [4] always fails. Many authors have already stressed the necessity for rigorous proofs of Coppersmith's method in the multivariate case. This is even more evident in light of these results.

1 Introduction

In this paper we consider the problem of breaking the RSA cryptosystem for short secret keys. An RSA public key is a pair (N, e) where $N = pq$ is a product of two n-bit primes. The corresponding secret key d is chosen such that it satisfies the equation $ed = 1 \bmod \frac{\phi(N)}{2}$, where $\phi(N) = (p-1)(q-1)$.

The first result showing that RSA is insecure, if the secret key is too small, is due to Wiener. In 1990, Wiener [20] showed that $d < \frac{1}{3}N^{0.25}$ leads to a polynomial time attack on the RSA system. Wiener's method is based on continued fractions. Basically, Wiener showed that d is the denominator of some convergent of the continued fraction expansion of e/N. A variant of Euclid's algorithm computes the continued fraction expansion of a number. Since N, e both are public, this shows that d can be computed efficiently from the public key (N, e).

Recently, Boneh and Durfee [4] proposed an attack on RSA, that shows that RSA is insecure provided $d < N^{0.292}$. Unlike Wiener's attack, the attack by Boneh and Durfee is a heuristic. It builds upon Coppersmith's result for finding small solutions of modular polynomial equations [6]. Coppersmith' method for the univariate case is rigorous but the proposed generalization for the multivariate case is a heuristic. More precisely, Boneh and Durfee show that for a small secret key d, the number $s = -\frac{p+q}{2}$ can be found as a small solution to some modular bivariate polynomial equation. Once s is known, one can immediately solve the equations $s = -\frac{p+q}{2}$ and $N = pq$ for the unknowns p and q. Using Coppersmith's method, which in turn is based on the famous L^3-lattice reduction algorithm, Boneh and Durfee reduce the problem of finding s to finding a common root of two bivariate polynomials $f(x, y), g(x, y)$ over the integers. As proposed by Coppersmith, finding a common root of f, g is done by first computing the resultant $r(y)$ of f, g with respect to the variable x. Provided $r \not\equiv 0$, the parameter s, and hence the factorization, can be found by computing the roots (over $\mathbb{Z}$) of r. Unfortunately, this method, as well as any other method based on Coppersmith's approach for multivariate polynomials[1], fails, if the resultant r is identically 0. As it has never been proved that $r \not\equiv 0$, the Boneh/Durfee approach is heuristic.

In this paper we study the method by Boneh and Durfee in more detail. In Section 4, we propose a new lattice for cryptanalysing low secret exponent RSA with $d < N^{0.290}$. The new approach uses the same heuristical assumption as Boneh/Durfee. Although the new attack does not improve the bound $d < N^{0.292}$ of Boneh and Durfee [4], it has several advantages. First, the lattice dimension is reduced. Therefore, in practice we are able to get closer to the theoretical bounds. Second, the new lattice basis is triangular. This leads to rather simple proofs. Third, the new lattice basis takes advantage of special properties of the lattice vectors. We believe that some of our structural results in Section 4 can be applied to other applications of Coppersmith's method as well.

Actually, Boneh and Durfee present three different variations of the Coppersmith methodology to break RSA versions with small secret exponent d. The first one works for $d < N^{1/4}$, hence this variant basically reproduces Wiener's result. The second variation of Boneh and Durfee works for $d < N^{0.284}$. Finally they have a method that works for d up to $N^{0.292}$.

We made the experimental observation, that the first method of Boneh and Durfee, supposed to work for $d < N^{1/4}$ always failed. In fact, in all experiments the resultant r mentioned above was identically zero. Although one cannot recover the factorization by resultant computation, we show that RSA with secret key $d < \frac{1}{3}N^{1/4}$ can be broken using lattice reduction in dimension 2. In fact, we show that for an appropriately chosen lattice, a shortest vector in the lattice immediately reveals the secret key d.

Since we have not found examples where the other two variants for $d < N^{0.284}$ and $d < N^{0.292}$ described by Boneh and Durfee fail, this observation in no way invalidates the results of Boneh and Durfee. On the other hand, this is to our knowledge the first case mentioned in literature, that an application of Coppersmith's approach fails in general. Some authors [6, 14] already pointed out that the heuristic must fail in some cases, but no general failure has been reported for real applications of the method.

Although we are not quite able to rigorously analyze the Boneh and Durfee method for $d < N^{1/4}$, in Section 5 we prove several results that almost completely explain the behavior observed in experiments. Many authors already stressed the necessity of a rigorous analysis of methods based on Coppersmith's approach in the multivariate case. This is even more evident in light of our results.

In Section 6 we give experimental results for our new attack on RSA with short secret key d. We carried out cryptanalysis of secret keys up to $d \leq N^{0.278}$. We also compared our experimental results with the experimental results of Boneh and Durfee. In [3], they only provided examples with $d \leq N^{0.265}$. In all cases we considered, our method was faster.

[1] This includes among others [1, 4, 8, 12]

2 The Boneh-Durfee Lattice

In this section we review the lattice attack by Boneh and Durfee on low exponent RSA. For an introduction into lattice theory and lattice basis reduction, we refer to the textbooks [9, 17]. Descriptions of Wiener's RSA attack and the method of Coppersmith can be found in [20, 6]. For a good overview of RSA attacks, we refer to a survey article of Boneh [2].

Let $d < e^{\delta}$. We assume that the size of e is in the order of the size of N. If e is smaller, the attack of Boneh and Durfee becomes even more effective (see [4], section 5).
All known attacks on RSA with short secret exponent focus on the identity

$$ed = 1 \bmod \frac{\phi(N)}{2} \quad \Leftrightarrow \quad ed + k\left(\frac{N+1}{2} + s\right) = 1, \tag{1}$$

where $k \in \mathbb{Z}$, $s = -\frac{p+q}{2}$ and d are unknown quantities. Since $e < \frac{\phi(N)}{2}$, we obtain $k < d$. Boneh and Durfee [4] look at equation (1) modulo e.

$$k\left(\frac{N+1}{2} + s\right) - 1 = 0 \bmod e$$

They define the polynomial

$$f(x, y) = x(A + y) - 1$$

with $A = \frac{N+1}{2}$. Let $X = e^{\delta}$ and $Y = e^{0.5}$. We know, that f has a root $(x_0, y_0) = (k, s)$ modulo e, that satisfies $|x_0| < X$ and $|y_0| < Y$. To transform the modular equation into an equation over the integers, Boneh/Durfee use a theorem of Howgrave-Graham [11]. Given a polynomial $p(x, y) = \sum_{i,j} a_{i,j} x^i y^j$, we define the norm $\|p(x, y)\|^2 = \sum_{i,j} a_{i,j}^2$.

Theorem 1 (Howgrave-Graham [11]). *Let $p(x, y)$ be a polynomial which is a sum of at most w monomials. Suppose that $p(x_0, y_0) = 0 \bmod e^m$ for some positive integer m, where $|x_0| < X$ and $|y_0| < Y$. If $\|p(xX, yY)\| < e^m/\sqrt{w}$, then $p(x_0, y_0) = 0$ holds over the integers.*

Next, Boneh and Durfee define polynomials

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

for a given positive integer m.

In the sequel, the polynomials $g_{i,k}$ are referred to as x-shifts and analogously the polynomials $h_{j,k}$ are referred to as y-shifts. By construction, the point (x_0, y_0) is a root of all these polynomials modulo e^m. Thus, we can apply Howgrave's theorem and search for a small norm linear combination of polynomials $g_{i,k}(xX, yY)$ and $h_{j,k}(xX, yY)$. This is done by using the L^3 lattice reduction algorithm. The goal is to construct a lattice that is guaranteed to contain a vector shorter than $e^m/\sqrt{w}$.

Boneh and Durfee suggest to build the lattice spanned by the coefficient vectors of the polynomials $g_{i,k}, h_{j,k}$ for certain parameters i, j and k. For each $k = 0, \ldots, m$, they use the x-shifts $g_{i,k}(xX, yY)$ for $i = 0, \ldots, m - k$. Additionally, they use the y-shifts $h_{j,k}$ for $j = 0, \ldots, t$ for some parameter t.

In the sequel, we call the lattice constructed by Boneh and Durfee the lattice L_{BD}. The basis for L_{BD} is denoted by B_{BD}. The lattice L_{BD} is spanned by the row vectors of B_{BD}. Since the lattice depends on the parameters m and t, we sometimes refer to the parameters by $B_{BD}(m,t)$ to clarify notation.

It is easy to see, that the basis vectors of lattice L_{BD} form a triangular matrix. We give an example of the lattice basis for the parameter choice $m = 2$ and $t = 1$.

$$
B_{BD}(2,1) = \left[\begin{array}{c|c|cc|ccc|ccc}
 & 1 & x & xy & x^2 & x^2y & x^2y^2 & y & xy^2 & x^2y^3 \\
\hline
e^2 & e^2 & & & & & & & & \\
\hline
xe^2 & & e^2X & & & & & & & \\
fe & -e & eAX & eXY & & & & & & \\
\hline
x^2e^2 & & & & e^2X^2 & & & & & \\
xfe & & -eX & & eAX^2 & eX^2Y & & & & \\
f^2 & 1 & -2AX & -2XY & A^2X^2 & 2AX^2Y & X^2Y^2 & & & \\
\hline\hline
ye^2 & & & & & & & e^2Y & & \\
yfe & & & eAXY & & & & -eY & eXY^2 & \\
yf^2 & & & -2AXY & & A^2X^2Y & 2AX^2Y^2 & Y & -2XY^2 & X^2Y^3
\end{array}\right]
$$

Boneh and Durfee showed for $\delta < 0.284$, one can find m, t such that an L^3-reduced basis of L_{BD} contains vectors short enough to apply Howgrave's theorem and factor the modulus N. This was improved in the same paper to $\delta < 0.292$ by using non-triangular lattice bases. This is up to now the best bound for cryptanalysis of low secret exponent RSA. The attack works under the assumption that polynomials obtained from two sufficiently short vectors in the reduced basis have a non-vanishing resultant. Although heuristic, no failure of the method for sufficiently large δ is known.

Boneh and Durfee also argue that using $t = 0$, that is only x-shifts are used to construct a lattice basis, one obtains already an attack working for $\delta < 0.25$. This reproduces Wiener's result. However, experiments show that the method of Boneh and Durfee never works when using only x-shifts. In Section 5, we will explain why this is the case. Of course, this failure of the Boneh/Durfee method in the special case where only x-shifts are used does not affect the method in general. It only points out that one has to be careful when using Coppersmith's heuristic in the multivariate case.

3 Notations

Since the lattice L_{BD} defined in Section 2 is the starting point of our further constructions, we introduce some notations on the rows and columns of the lattice basis B_{BD}.

We refer to the coefficient vectors of the polynomials $g_{i,k}(xX, yY)$ as the X-block. The X-block is further divided into $X_l, l = 0, \dots, m$, blocks, where the block X_l consist of the $l+1$ coefficient vectors of $g_{i,k}$ with $i + k = l$. These $l + 1$ vectors are called $X_{l,k}$, that is the k-th vectors in the X_l block is the coefficient vector of $g_{l-k,k}$.

The coefficient vectors of the polynomials $h_{j,k}$ form the Y-block. We define the Y_j block as the block of all $m + 1$ coefficient vectors of polynomials that are shifted by y^j. The k-th vector in the block Y_j is called $Y_{j,k}$, it is identical to the coefficient vector of $h_{j,k}$.

Every column in the basis B_{BD} is labeled by a monomial $x^i y^j$. All column vectors with label $x^l y^j$, $l \geq j$, form the $X^{(l)}$ column block. Analogously, we define the $Y^{(l)}$ column block to consist of all column vectors labeled with $x^i y^{i+l}$.

In the example in Section 2, the horizontol lines divide the basis $B_{BD}(2,1)$ into the blocks X_1, X_2, X_3 and Y_1. Analogously, the vertical lines divide $B_{BD}(2,1)$ into the column blocks $X^{(1)}$, $X^{(2)}$, $X^{(3)}$ and $Y^{(1)}$. In this example, the basis entry in row $Y_{1,2}$ and column x^2y is A^2X^2Y.

4 A new method for all $\delta < 0.290$

We introduce an alternative method for factoring the modulus N if $d < N^{0.290}$. This does not improve the bound $\delta < 0.292$ given by Boneh and Durfee. However, it has several advantages compared to their approach.

First, our method significantly reduces the lattice dimension as a function of m and t. The practical implication is that we are able to get closer to the theoretical bound. We give experimental results for $\delta > 0.265$. Second, our proofs are simple. As opposed to the Boneh/Durfee lattices for $\delta < 0.292$, the lattice bases we use in the attack for $\delta < 0.290$ remain triangular. Hence, determinant computations are simple. Third, our construction makes use of structural properties of the underlying polynomials. Thus, it should apply also to other lattice constructions using these polynomials.

Construction of the new lattice L with basis B

1. Choose lattice parameters m and t and build the Boneh-Durfee lattice basis $B_{BD}(m,t)$ as explained in Section 2.
2. In the Y_t block of the basis B_{BD} remove every vector except for the last vector $Y_{t,m}$, in the Y_{t-1} block remove every vector except for the last two vectors $Y_{t,m-1}$ and $Y_{t,m}$, and so on. Finally, in the Y_1 block remove every vector except for the last t vectors $Y_{m-t+1}, \ldots, Y_m$.
3. Remove every vector in the X-block except for the vectors in the $t+1$ blocks X_{m-t}, $X_{m-t+1}, \ldots, X_m$.
4. Delete columns in such a way that the resulting basis is again triangular. This is, remove all column blocks $X^{(0)}, X^{(1)}, \ldots, X^{(m-t-1)}$. Furthermore in the column block $Y^{(l)}$, $l = 1, \ldots, t$, remove the columns labeled with $x^i y^{i+l}$ for $0 \le i < m - t + l$.

This construction leads to a triangular basis B of a new lattice L, which will be used in our approach. Since B depends on m and t, we sometimes write $B(m,t)$.

As opposed to Boneh and Durfee, we do not integrate more y-shifts to improve the bound $\delta < 0.284$, instead we remove some x-shifts.

Remark 1 *In our construction, we take the pattern $(p_0, p_1, \ldots, p_t) = (1, 2, \ldots, t+1)$. That is, we take the last p_i, $0 \le i < t$ vectors from the Y_{t-i} block and the last p_t X-blocks and delete columns appropriately. The proofs in this section easily generalize to every strictly increasing pattern $(p_0, p_1, \ldots, p_t)$, $p_0 < p_1 < \cdots < p_t$. This includes among others the pattern used by Boneh/Durfee [4] to show the bound $d < N^{0.292}$. We give the proof of this generalization in the full version of the paper.*

Applying the construction to the example given in Section 2, we obtain the following lattice basis of L with parameters $m = 2$ and $t = 1$.

$$
B(2,1) = \left[\begin{array}{c|cc|ccc|c}
 & x & xy & x^2 & x^2y & x^2y^2 & x^2y^3 \\
\hline
xe^2 & e^2X & & & & & \\
fe & eAX & eXY & & & & \\
\hline
x^2e^2 & & & e^2X^2 & & & \\
xfe & -eX & & eAX^2 & eX^2Y & & \\
f^2 & -2AX & -2XY & A^2X^2 & 2AX^2Y & X^2Y^2 & \\
\hline\hline
yf^2 & & -2AXY & & A^2X^2Y & 2AX^2Y^2 & X^2Y^3
\end{array}\right]
$$

Let $\bar{B}$ be the non-triangular basis we obtain after Step 3 of the construction. That is, $\bar{B}$ consists of the remaining basis vectors of B_{BD} in the construction after removing row vectors but without removing columns. The lattice spanned by the row vectors of $\bar{B}$ is called $L_{\bar{B}}$. We adopt the notations of Section 3 for the rows and columns of B and $\bar{B}$. For example, the row vector $X_{l,k}$ of B is the coefficient vector of $g_{l-k,k}$, where we removed all the entries specified in Step 4 of the construction. In the basis $B(2,1)$ above, the row vector $X_{2,0}$ is the vector $(0, 0, e^2X^2, 0, 0, 0)$.

We call a column vector x^iy^j that appears in the basis $\bar{B}$ but not in the basis B a *removed column* of B. The bases B and $\bar{B}$ are constructed using the same coefficient vectors, where in B certain columns are removed. Having a vector $u = \sum_{b \in B} c_b b$ in the span of B, one can compute the corresponding linear combination $\bar{u} = \sum_{b \in \bar{B}} c_b b$ of vectors in $\bar{B}$ with the same coefficients c_b. Hence, the vector dimension of $\bar{u}$ is larger than the vector dimension of u. One can regard the additional vector entries in $\bar{u}$ as a reconstruction of the vector entries of u in the removed columns. Therefore, we call $\bar{u}$ the *reconstruction vector* of u.

The row vectors $X_{l,k}$ ($l = m-t, \ldots, m; k \le l$) and $Y_{j,k}$ ($j = 1, \ldots, t; k = m-t+j, \ldots, m$) form the basis B. These vectors are no longer the coefficient vectors of the polynomials $g_{l-k,k}(xX, yY)$ and $h_{j,k}(xX, yY)$, respectively, since we remove columns in Step 4 of the construction. However in order to apply Howgrave's theorem, we must ensure that we construct a linear combination of bivariate polynomials that evaluates to zero modulo e^m at the point $(x_0, y_0) = (k, s)$. Hence, we still have to associate the rows $X_{l,k}$ and $Y_{j,k}$ with the polynomials $g_{l-k,k}$ and $h_{j,k}$. The basis vectors of $\bar{B}$ represent the coefficient vectors of these polynomials. Therefore, after finding a small vector $u = \sum_{b \in B} c_b b$ in L, we compute the reconstruction vector $\bar{u} = \sum_{b \in \bar{B}} c_b b$ in $L_{\bar{B}}$. That is, we reconstruct the entries in the removed columns. Once the reconstruction vectors of two sufficiently short vectors in L are computed, the rest of our method is the same as in the Boneh/Durfee method.

In the remainder of this section we show that short vectors u in L lead to short reconstruction vectors $\bar{u}$ in $L_{\bar{B}}$. To prove this, we first show that removed columns of B are small linear combinations of column vectors in B. We give an example for the removed column x^0y^0 in $B(2,1)$. Applying the construction in the following proof of Lemma 2, we see that this column is a linear combination of the columns x^1y^1 and x^2y^2 in B.

$$
\left(\begin{array}{c} 0 \\ -e \\ \hline 0 \\ 0 \\ 1 \\ \hline 0 \end{array}\right) = -\frac{1}{XY} \left(\begin{array}{c} 0 \\ eXY \\ \hline 0 \\ 0 \\ -2XY \\ \hline -2AXY \end{array}\right) - \frac{1}{X^2Y^2} \left(\begin{array}{c} 0 \\ 0 \\ \hline 0 \\ 0 \\ X^2Y^2 \\ \hline 2AX^2Y^2 \end{array}\right)
$$

Lemma 2 *All removed columns in the column blocks $X^i, i < m-t$, are linear combinations of columns in B. Moreover, in these linear combinations, the coefficient for a column vector in $X^{(l)}, l \geq m-t$, can be bounded by $\frac{1}{(XY)^{l-i}} \cdot c$, where c depends only on m and t.*

Proof: If $x^i y^j$ is a removed column of B, we show that $x^i y^j$ is a linear combination of columns $x^{i+1}y^{j+1}$, ..., $x^m y^{m-i+j}$. If $x^{i+1}y^{i+1}$ is a removed column, we can repeat the argument to show that $x^{i+1}y^{i+1}$ is a linear combination of the remaining columns $x^{i+2}y^{j+2}$, ..., $x^m y^{m-i+j}$. Continuing in this way until all removed columns have been represented as linear combinations of columns in B, proves the lemma. Hence, it suffices to prove the following claim.

Claim 1 *If $x^i y^j$ is a removed column of B, then $x^i y^j$ is a linear combination of the columns $x^{i+1}y^{j+1}$, $x^{i+2}y^{j+2}$,..., $x^m y^{m-i+j}$, where the coefficient of column $x^{i+b}y^{j+b}, b = 1, \ldots, m-i$, is given by*

$$-\frac{1}{(XY)^b}\binom{j+b}{j}.$$

Note, that the coefficient $c_b = \binom{j+b}{j}$ depends only on m and t, since i, j depend on m and t.

We will prove Claim 1 by showing that for each row in $B(m,t)$ the entry of the column $x^i y^j$ in this row is a linear combination of the entries of the columns $x^{i+b}y^{j+b}$ in this row, with the coefficients as in the claim. We prove this for the rows in the X-block and Y-block separately.

Let $X_{l,k}$ be a row in block X_l, where $l \geq m-t$. The coefficients in this row are the coefficients of the polynomial $e^{m-k}x^{l-k}f^k(xX, yY)$. By definition of f this polynomial is

$$e^{m-k}x^{l-k}f^k(xX,yY) = e^{m-k}\sum_{p=0}^{k}\sum_{q=0}^{p}(-1)^{k+p}\binom{k}{p}\binom{p}{q}A^{p-q}X^pY^qx^{p+l-k}y^q. \qquad (2)$$

To obtain the coefficient of $x^{i+b}y^{j+b}$ in $e^{m-k}x^{l-k}f^k(xX, yY)$, we set $p = i-l+k+b$ and $q = j+b$. Hence, this coefficient is given by

$$\begin{aligned} & e^{m-k}(-1)^{i-l+b}\binom{k}{i-l+k+b}\binom{i-l+k+b}{j+b}A^{i-l+k-j}X^{i-l+k+b}Y^{j+b} \\ &= e^{m-k}A^{i-l+k-j}X^{i-l+k}Y^j(-1)^{i-l}(-1)^b\binom{k}{i-l+k+b}\binom{i-l+k+b}{j+b}(XY)^b. \end{aligned}$$

We can ignore the factor $e^{m-k}A^{i-l+k-j}X^{i-l+k}Y^j(-1)^{i-l}$, common to all entries in row $X_{l,k}$ in the columns $x^{i+b}y^{j+b}$. Then Claim 1 restricted to row $X_{l,k}$ reads as

$$\binom{k}{i-l+k}\binom{i-l+k}{j} = \sum_{b=1}^{m-i}(-1)^{b+1}\frac{1}{(XY)^b}\binom{j+b}{j}\binom{k}{i-l+k+b}\binom{i-l+k+b}{j+b}(XY)^b$$

Since the binomial coefficient $\binom{k}{i-l+k+b}$ is non-zero only for $k \geq i-l+k+b$, we only have to sum up to $b \leq l-i$. Substituting $i-l+k$ by i' yields

$$\binom{k}{i'}\binom{i'}{j} = \sum_{b=1}^{k-i'}(-1)^{b+1}\binom{j+b}{j}\binom{k}{i'+b}\binom{i'+b}{j+b}. \qquad (3)$$

Subtracting the left-hand side, Claim 1 restricted to row $X_{l,k}$ reduces to

$$0 = \sum_{b=0}^{k-i'} (-1)^{b+1} \binom{j+b}{j} \binom{k}{i'+b} \binom{i'+b}{j+b}. \tag{4}$$

One checks that

$$\binom{j+b}{j} \binom{k}{i'+b} \binom{i'+b}{j+b} = \frac{k!}{(k-i')!j!(i'-j)!} \binom{k-i'}{b}.$$

This shows

$$\sum_{b=0}^{k-i'} (-1)^{b+1} \binom{j+b}{j} \binom{k}{i'+b} \binom{i'+b}{j+b} = -\frac{k!}{(k-i')!j!(i'-j)!} \sum_{b=0}^{k-i'} (-1)^b \binom{k-i'}{b}.$$

Since $\sum (-1)^b \binom{k-i'}{b} = (1+(-1))^b = 0$ we get equation (4).

In the same manner, Claim 1 is proved for the Y-block. Let $Y_{l,k}$ be a row in block Y_l. Analogously to equation (2), we get

$$e^{m-k} y^l f^k(xX, yY) = e^{m-k} \sum_{p=0}^{k} \sum_{q=0}^{p} (-1)^{k+p} \binom{k}{p} \binom{p}{q} A^{p-q} X^p Y^q x^p y^{q+l}.$$

We obtain the coefficients of $x^{i+b} y^{j+b}$ in $e^{m-k} y^l f^k(xX, yY)$ by setting $p = i+b$ and $q = j-l+b$. Again, we ignore the common factors in e, A, X and Y. Now, Claim 1 for $Y_{l,k}$ reduces to

$$\binom{k}{i} \binom{i}{j-l} = \sum_{b=1}^{m-i} (-1)^{b+1} \binom{j+b}{j} \binom{k}{i+b} \binom{i+b}{j-l+b}$$

We only have to some up to $b \le k-i$, because the factor $\binom{k}{i+b}$ is zero for $k < i+b$. Substituting $j-l$ by j and i by i' yields equation (3). This concludes the proof. $\square$

Lemma 3 *Every removed column vector $x^i y^{i+l}, i < m-t+l$, is a linear combination of the columns in the column block $Y^{(l)}$ of B. In this linear combination, the coefficient for a column vector $x^k y^{k+l}, k \ge m-t+l$, can be bounded by $\frac{1}{(XY)^{k-i}} \cdot c$, where c depends only on m and t.*

Proof. Analogously to the proof of Lemma 2. Therefore we omit it.

Theorem 2. *Let $u = \sum_{b \in B} c_b b$ be a linear combination of vectors in B with $\|u\| < e^m$. For fixed m and t and for every removed column $x^i y^j$ in the $X^{(i)}$ block $(0 \le i < m-t)$, the entry $x^i y^j$ in the reconstruction vector $\bar{u} = \sum_{b \in \bar{B}} c_b b$ can be bounded by $O\left(\frac{e^m}{(XY)^{m-t-i}}\right)$.*

Proof: Consider a removed column $x^i y^j$. Let $v = (v_1, v_2, \ldots, v_n)^T$ be the column vector $x^i y^j$ in $\bar{B}$, where the entries are multiplied by the coefficients c_b. We want to show that $|\sum_{k=1}^n v_k| = O(\frac{e^m}{(XY)^{m-t-i}})$. This will prove the theorem.

Apply Lemma 2 and write v as a linear combination of the t+1 columns $x^{m-t}y^{m-t-i+j}$, $\ldots$, $x^m y^{m-i+j}$ in B, where again the entries in each of the $t+1$ vectors are multiplied by the coefficients c_b. Call these columns $w_i = (w_{i,1}, \cdots, w_{i,n})^T$ for $i = 0, \ldots, t$. Applying Lemma 2 yields

$$v = \frac{d_0}{(XY)^{m-t-i}} w_0 + \frac{d_1}{(XY)^{m-t-i+1}} w_1 + \cdots + \frac{d_t}{(XY)^{m-i}} w_t$$

According to Lemma 2, the d_i are constant for fixed m and t. By assumption $\|u\| < e^m$. Hence, all components of u are less than e^m. From this, we obtain $|\sum_k w_{i,k}| < e^m$. This implies

$$\begin{aligned}
\left|\sum_k v_k\right| &= \left|\frac{d_0}{(XY)^{m-t-i}} \sum_k w_{0,k} + \cdots + \frac{d_t}{(XY)^{m-i}} \sum_k w_{t,k}\right| \\
&\le \left|\frac{d_0}{(XY)^{m-t-i}} \sum_k w_{0,k}\right| + \cdots + \left|\frac{d_t}{(XY)^{m-i}} \sum_k w_{t,k}\right| \\
&\le \left|\frac{d_0}{(XY)^{m-t-i}} e^m\right| + \cdots + \left|\frac{d_t}{(XY)^{m-i}} e^m\right| \\
&= O\left(\frac{e^m}{(XY)^{m-t-i}}\right) + \cdots + O\left(\frac{e^m}{(XY)^{m-i}}\right)
\end{aligned}$$

Therefore, $|\sum_k v_k|$ can be bounded by $O\left(\frac{e^m}{(XY)^{m-t-i}}\right)$. □

Theorem 3. *Let $u = \sum_{b \in B} c_b b$ be a linear combination of vectors in B with $\|u\| < e^m$. For fixed m and t and for every removed column $x^i y^{i+l}$ in the $Y^{(l)}$ block ($0 \le i < m-t+l, 1 \le l \le t$), the entry $x^i y^{i+l}$ in the reconstruction vector $\bar{u} = \sum_{b \in \bar{B}} c_b b$ can be bounded by $O\left(\frac{e^m}{(XY)^{m-t+l-i}}\right)$.*

Proof. Analogously to the proof of Theorem 2. The proof is omitted.

From Theorems 2 and 3, we can conclude that if we use the reconstruction vector $\bar{u}$ instead of the short vector u, we do not enlarge the norm significantly. This shows the correctness of our approach.

Corollary 4 *Let $u = \sum_{b \in B} c_b b$ with $\|u\| < e^m$ be a vector in L. Then the reconstruction vector $\bar{u} = \sum_{b \in \bar{B}} c_b b$ satisfies $\|\bar{u}\| < e^m + O(\frac{e^m}{XY})$.*

4.1 Computation of the new bound

Since the lattice basis for L is triangular, computing the determinant of lattice L is easy. We do not carry out the computation. Manipulating the expressions for the determinant is straightforward, but requires tedious arithmetic.

The lattice dimension w equals the number of vectors in the blocks $X_{m-t}, \dots, X_m$ and $Y_1, \dots, Y_t$.

$$w = \sum_{i=m-t}^{m} (i+1) + \sum_{i=1}^{t} i = (m+1)(t+1)$$

Notice, that we have $w = (m+1)(m+2)/2 + t(m+1)$ for the lattice L_{BD}.

We compute the determinant $\det(L)$ as a function of e, m, t and δ. We find the optimal t as a function of m, δ by elementary calculus. Analogously to the method of Boneh/Durfee, we solve the equation

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

for the maximal value of δ. This leads to the bound

$$\delta < \frac{\sqrt{6}-1}{5} \approx 0.290.$$

5 A case where the heuristic fails

As mentioned before, if L_{BD} is constructed using only x-shifted polynomials $g_{i,k}$ then the Boneh/Durfee method always failed in our experiments. More precisely, the polynomials we obtained from the two shortest vectors in an L^3-reduced basis for L_{BD} led to two polynomials whose resultant with respect to x was identically 0. We want to explain this phenomenon.

Using the construction of Section 4 in the special case of $t = 0$ and $m = l_1$, the lattice L consists only of the vectors in the block X_{l_1} with the columns in $X^{(l_1)}$. A simple determinant computation shows, that for every X_{l_1} block there is a linear combination of vectors in block X_{l_1} that is shorter than e^m provided $\delta < 0.25$.

Moreover, unless a combination of vectors in block X_{l_2} is much shorter than e^m (according to Theorem 2 it must be of size $O(\frac{e^m}{XY})$), combinations of vectors from different blocks X_{l_1}, X_{l_2} can not be shorter than vectors obtained as combinations of vectors from a single block X_{l_1}. Although not a rigorous proof, this explains the following observation. In our experiments every vector in an L^3-reduced basis for $B_{BD}(m, 0)$ was a combination of basis vectors from a single block X_{l_1}[2].

Now assume that we compute the resultant of two polynomials p_1, p_2, obtained from vectors v_1, v_2 whose length is smaller than $e^m/\sqrt{w}$ and that are linear combinations of basis vectors in X_{l_1} and X_{l_2}, respectively. By construction of L_{BD} and Howgrave's theorem (Theorem 1), p_1 and p_2 have a common root $(x_0, y_0) = (k, s)$. The following theorem shows that in this case the Boneh/Durfee attack fails.

Theorem 4. *Let $p_1(x, y)$ and $p_2(x, y)$ be polynomials that are non-zero linear combinations of the X_{l_1} and X_{l_2} block, respectively. If $p_1(x_0, y_0) = p_2(x_0, y_0) = 0$ for at least one pair $(x_0, y_0) \in \mathbb{C} \times \mathbb{C}$ then* $\mathrm{Res}_x(p_1, p_2) = 0$.

[2] In fact, the following was true for arbitrary L_{BD}, even those constructed using y-shifts: Every vector in an L^3-reduced basis for L_{BD} that depended only on basis vectors in the X-block was a combination of basis vectors from a single block X_{l_1}

Proof: Write p_1 and p_2 as linear combinations

$$p_1(x,y) = \sum_{i=0}^{l_1} c_i x^{l_1-i} f^i(x,y) e^{m-i} \ , \ p_2(x,y) = \sum_{i=0}^{l_2} d_i x^{l_2-i} f^i(x,y) e^{m-i}.$$

We know $l_1, l_2 > 0$, since $p_1(x_0,y_0) = p_2(x_0,y_0) = 0$ for at least one pair (x_0,y_0). If $c_0 = d_0 = 0$, then f is a common factor of p_1 and p_2 and $\mathrm{Res}_x(p_1,p_2) = 0$. Hence, we may assume $c_0 \neq 0$ or $d_0 \neq 0$.

Let $r(y) = \mathrm{Res}_x(p_1,p_2)$ be the resultant of p_1, p_2 with respect to the variable x. Let $T = \{z \in \mathbb{C} \mid r(z) = 0\}$ be the set of roots of $r(y)$. Next, define S as

$$S = \{y \in \mathbb{C} \mid \text{ there is an } x \in \mathbb{C} \text{ such that } p_1(x,y) = p_2(x,y) = 0\}.$$

S is the projection of the common roots of p_1, p_2 onto the second coordinate. It is well-known that $S \subseteq T$ (see for example [7]). Our goal is to show, that $|S| = \infty$. Then $|T| = \infty$ as well, and $r(y) = \mathrm{Res}_x(p_1,p_2) = 0$ as stated in the theorem.
To show that $|S| = \infty$, we first perform the transformation τ defined by

$$\tau(x,y) = (x',y) \ \text{ with } \ (x',y) = \left(\frac{x}{f(x,y)}, y\right).$$

We obtain

$$x' = \frac{x}{x(A+y)-1} = \frac{1}{A+y-\frac{1}{x}}.$$

This implies $\frac{1}{x'} = A + y - \frac{1}{x}$ and $\frac{1}{x} = A + y - \frac{1}{x'}$. From the second equality we get $x = \frac{x'}{x'(A+y)-1} = \frac{x'}{f(x',y)}$. We also get

$$f(x',y) = \frac{x}{x(A+y)-1} \cdot (A+y) - 1 = \frac{1}{x(A+y)-1} = \frac{1}{f(x,y)}.$$

Applying the transformation to the polynomials p_1, p_2 gives rational polynomials q_1, q_2, where

$$q_1(x',y) = f^{-l_1}(x',y) \sum_{i=0}^{l_1} c_i x'^{l_1-i} e^{m-i}, \quad q_2(x',y) = f^{-l_2}(x',y) \sum_{i=0}^{l_2} d_i x'^{l_2-i} e^{m-i}.$$

Hence q_1, q_2 are of the form $q_1(x',y) = \frac{1}{f^{l_1}} g_1(x'), q_2(x',y) = \frac{1}{f^{l_2}} g_2(x')$, for polynomials g_1, g_2 that depend only on x'.
Let

$$S' = \{y \in \mathbb{C} \mid \text{ there is an } x \in \mathbb{C} \text{ such that } q_1(x,y) = q_2(x,y) = 0\}.$$

If g_1, g_2 do not have a common root, then $S' = \emptyset$. On the other hand, if g_1, g_2 have a common root x then $S' = \mathbb{C} \backslash \{\frac{1}{x} - A\}$, since $y = \frac{1}{x} - A$ is the only value y for which $f(x,y) = 0$. In particular, either $S' = \emptyset$ or $|S'| = \infty$. In order to show that $|S'| = \infty$, it suffices to show that there is at least one $y \in S'$.

In order to prove the theorem, it suffices to show that the transformation τ induces a bijective mapping of the common roots of p_1, p_2 onto the common roots of q_1, q_2. By assumption, p_1 and p_2 share the common root (x_0, y_0). Then, $\tau(x_0, y_0)$ is a common root of

q_1, q_2. This implies $y_0 \in S'$ and therefore $|S'| = \infty$. By the bijectivity of τ, we get $|S| = \infty$ as well.

Whenever defined, the transformation τ is the inverse of itself. This implies that τ is bijective on its domain, that is on all points (x, y) where $f(x, y) \neq 0$. Hence, a common root (x, y) of p_1, p_2 is not in the domain of τ iff (x, y) is a root of f. So assume $(x, y) \in \mathbb{C} \times \mathbb{C}$ is such that $f(x, y) = 0$. Then all term in p_1 and p_2 vanish except for $i = 0$. We get $p_1(x, y) = c_0 x^{l_1} e^m$ and $p_2(x, y) = d_0 x^{l_2} e^m$. But $f(x, y) = x(A + y) - 1 = 0$ implies $x \neq 0$. In this case, p_1 and p_2 do not have a common root because either $c_0 \neq 0$ or $d_0 \neq 0$. Hence p_1, p_2, f do not have a common root and the transformation τ induces a bijective mapping of the common roots of p_1, p_2 onto the common roots of q_1, q_2. This concludes the proof of the theorem. □

More can be said about the Boneh/Durfee attack when L_{BD} is constructed using only x-shifts. In the experiments we carried out, an L^3-reduced basis of L_{BD} always contained a vector v depending only on the basis vectors in X_1. As usually, we denote the basis vectors in X_1 by $X_{1,0}, X_{1,1}$. The vector v was of the form $d \cdot X_{1,0} + k \cdot X_{1,1}$, where d is the secret key and k is defined by $ed = 1 - k\frac{\phi(N)}{2}$. Hence, v alone reveals the secret key.

This is explained by the following theorem. Consider the lattice L spanned by the rows of the (2×2) lattice basis

$$B(1,0) = \begin{bmatrix} eX & 0 \\ AX & XY \end{bmatrix}.$$

Theorem 5. *If we choose $Y = e^{1/2}$ and $X = 2e^{1/4}$ for the basis $B(1,0)$, then the coefficients of the shortest lattice vector equal the secret parameters k and d provided $d < \frac{1}{3}N^{1/4}$.*

Proof: We only sketch the proof idea. Details are given in the full version of the paper.

We show that for the shortest vector $u = c_1 X_{1,0} + c_2 X_{1,1}$ the quotient $\frac{c_1}{c_2}$ is a convergent in the continued fraction expansion of $\frac{A}{e}$. Furthermore, $\frac{c_1}{c_2}$ is the last convergent of $\frac{A}{e}$ whose denominator is less than $e^{1/4}$.

It can be shown using Wiener's argument, that $\frac{d}{k}$ is also the last convergent of $\frac{A}{e}$ with denominator less than $e^{1/4}$. This implies $\frac{c_1}{c_2} = \frac{d}{k}$.

□

6 Experiments

We implemented our new method and carried out several experiments on a Linux-PC with 550 MHz. The L^3 reduction was done using Victor Shoup's NTL library [18].

In every experiment, we found two vectors with norm smaller than $\frac{e^m}{\sqrt{w}}$. Interestingly in the experiments carried out, the reduced lattice basis contained not only two sufficiently small vectors, but all vectors in the L^3-reduced basis of L had about the same norm. This is a difference to the Boneh/Durfee lattice bases. The resultant of the corresponding polynomials was computed using the Maple computer algebra system. The resultant with respect to x was always a polynomial in y, and the root delivered the factorization of N. Our results compare well to those of Boneh and Durfee in the Eurocrypt paper [3].

Boneh/Durfee ran new experiments in [4], but used additional tricks to enlarge d by a few bits:

1. Lattice reduction with Schnorr's block reduction variant [16].
2. Use of Chebychev polynomials (a trick due to Coppersmith).
3. If $\|p(xX, yY)\| < c \cdot e^m/\sqrt{w}$, we know $|p(x_0, y_0)| < c \cdot e^m$ and $p(x_0, y_0) = 0 \bmod e^m$. Hence, we can guess $\gamma \in (-c, c)$ such that $p(x, y) + \gamma e^m$ satisfies $p(x_0, y_0) + \gamma e^m = 0$ over $\mathbb{Z}$.

These tricks apply to our method as well, but we did not implement them. Comparing instances with the same bitsize of p, q and the same δ as in [3], our algorithm was several times faster due to the reduced lattice dimension. The following table contains several running times we obtained. Where availabe, we also included the corresponding running times as provided in [3] (these running times were achieved on a 400 MHz SUN workstation).

p, q	δ	m	t	w	our running time	running time in [4]
1000 bits	0.265	4	2	15	6 minutes	45 minutes
3000 bits	0.265	4	2	15	100 minutes	300 minutes
3000 bits	0.269	5	2	18	8 hours	-
500 bits	0.270	6	2	21	19 minutes	-
500 bits	0.274	8	3	36	300 minutes	-
500 bits	0.2765	10	4	55	26 hours	-
500 bits	0.278	11	5	72	6 days	-

In all examples we chose d uniformly with $\delta \log(N)$ bits, until $\log_N(d)$ was δ within precision at least 10^{-4}. The running time measures only the time for L^3-reduction. With growing m and t, the time for resultant computation can take longer than reducing the lattice basis $B(m, t)$.

7 Acknowledgement

We want to thank Glenn Durfee for pointing out the additional tricks in Section 6 and the anonymous referees for their helpful comments.

References

1. D. Bleichenbacher, "On the Security of the KMOV public key cryptosystem", Proc. of Crypto '97
2. D. Boneh, "Twenty years of attacks on the RSA cryptosystem", Notices of the AMS, 1999
3. D. Boneh, G. Durfee, "Cryptanalysis of RSA with private key d less than $N^{0.292}$", Proc. Eurocrypt '99
4. D. Boneh, G. Durfee, "Cryptanalysis of RSA with private key d less than $N^{0.292}$", IEEE Trans. on Information Theory, vol. 46(4), 2000
5. H. Cohen, "A Course in Computational Algebraic Number Theory", Springer Verlag, 1996
6. D. Coppersmith, "Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities", Journal of Cryptology 10(4), 1997
7. D. Cox, J. Little, D. O'Shea, "Ideals, Varieties and Algorithms", Springer Verlag, 1992
8. G. Durfee, P. Nguyen, "Cryptanalysis of the RSA Schemes with Short Secret Exponent from Asiacrypt '99", Proc. of Asiacrypt '2000
9. M. Gruber, C.G. Lekkerkerker, "Geometry of Numbers", North-Holland, 1987

10. G.H. Hardy, E.M. Wright, "An Introduction to the Theory of Numbers", Oxford University Press, 1979
11. N. Howgrave-Graham, "Finding small roots of univariate modular equations revisited", Proc. of Cryptography and Coding, LNCS 1355, Springer-Verlag, 1997
12. C. Jutla, "On finding small solutions of modular multivariate polynomial equations", Proc. of Eurocrypt '98
13. A. Lenstra, H. Lenstra and L. Lovasz, "Factoring polynomials with rational coefficients", Mathematische Annalen, 1982
14. P. Nguyen, J. Stern, "Lattice Reduction in Cryptology: An Update", Algorithmic Number Theory Symposium ANTS-IV, 2000
15. R. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems", Communications of the ACM, volume 21, 1978
16. C.P. Schnorr, "A hierarchy of polynomial time lattice basis reduction algorithms", Theoretical Computer Science, volume 53, 1987
17. C.L. Siegel, "Lectures on the Geometry of Numbers", Springer Verlag, 1989
18. V. Shoup, Number Theory Library (NTL), http://www.cs.wisc.edu/~shoup/ntl
19. E. Verheul, H. van Tilborg, "Cryptanalysis of less short RSA secret exponents", Applicable Algebra in Engineering, Communication and Computing, Springer Verlag, vol. 8, 1997
20. M. Wiener, "Cryptanalysis of short RSA secret exponents", IEEE Transactions on Information Theory, vol. 36, 1990