Partial Key Exposure Attacks on RSA up to Full Size Exponents

Matthias Ernst[1], Ellen Jochemsz[2⋆],
Alexander May[1⋆], and Benne de Weger[2⋆]

[1] Faculty of Computer Science, Electrical Engineering and Mathematics,
University of Paderborn, 33102 Paderborn, Germany
{alder,alexx}@uni-paderborn.de
[2] Department of Mathematics and Computer Science,
Eindhoven University of Technology, Eindhoven, The Netherlands
{e.jochemsz,b.m.m.d.weger}@tue.nl

Abstract. We present several attacks on RSA that factor the modulus in polynomial time under the condition that a fraction of the most significant bits or least significant bits of the private exponent is available to the attacker. Our new attacks on RSA are the first attacks of this type that work up to full size public or private exponent.

Keywords: RSA, cryptanalysis, partial key exposure, lattice reduction, Coppersmith's method.

1 Introduction

There have been a number of attacks on RSA given a portion of the private key. These attacks are so-called partial key exposure attacks, where an attacker has some knowledge of the bits of the private key and uses it to break the system. The results are of practical interest, since implementations may leak bits of the private key, e.g. via side channel attacks.

In 1998, Boneh, Durfee and Frankel presented several partial key exposure attacks on RSA in [2]. Some of these attacks require knowledge of the least significant bits (LSBs) of the private exponent, others of the most significant bits (MSBs). Additionally, in their attacks, the public exponent must be relatively small. Wiener's attack [12] and the improvement by Boneh and Durfee [1] can be seen as partial key exposure attacks where the most significant bits of the private exponent are known to be equal to zero.

In [2] the question is posed whether there exist partial key exposure attacks on RSA that work for public exponents larger than the square root of the modulus. In 2003, Blömer and May [3] described a number of attacks that do allow larger

⋆ The work described in this paper has been supported in part by the European Commission through the IST Programme under Contract IST-2002-507932 ECRYPT. The information in this document reflects only the author's views, is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

public exponents, but not yet to the full size of the modulus. In this paper we present attacks for full size public exponent that work up to full size private exponent. Additionally, we present a new attack for full size private exponent that works up to full size public exponent.

Our attacks use Coppersmith's ideas of finding small roots of polynomials [4]. We look at variations on the RSA key equation over the integers, using Coppersmith's method of finding small integer roots, reformulated by Coron [5].

Our new results on known MSBs of d for small private exponent d and full size public exponent e are summarized in the following theorem.

Theorem 1 (MSB small d). *Under a common heuristic assumption concerning resultants, for every $\epsilon > 0$, there exists n_0 such that for every $n > n_0$, the following holds:*
Let $N = pq$ be an n-bit RSA-modulus, and p, q primes of bitsize $\frac{n}{2}$. Let $0 < \delta < \beta < 1$. Furthermore, let e, d satisfy $ed \equiv 1 \bmod \phi(N)$ with bitsize(e) $= n$ and bitsize(d) $= \beta n$. Given the $(\beta - \delta)n$ MSBs of d, N can be factored in polynomial time if:

- $\delta \leq \frac{5}{6} - \frac{1}{3}\sqrt{1+6\beta} - \epsilon$ *(Section 4.1.1), or*
- $\delta \leq \frac{3}{16} - \epsilon$ *and* $\beta \leq \frac{11}{16}$ *(Section 4.1.2), or*
- $\delta \leq \frac{1}{3} + \frac{1}{3}\beta - \frac{1}{3}\sqrt{4\beta^2 + 2\beta - 2} - \epsilon$ *and* $\beta \geq \frac{11}{16}$ *(Section 4.1.2).*

In the case of known MSBs for full size d and small e, we find an improvement of known results by [2] and [3] for $e \in [N^{\frac{1}{2}}, N]$. Our result is stated in the theorem below.

Theorem 2 (MSB small e). *Under a common heuristic assumption concerning resultants, for every $\epsilon > 0$, there exists n_0 such that for every $n > n_0$, the following holds:*
Let $N = pq$ be an n-bit RSA-modulus, and p, q primes of bitsize $\frac{n}{2}$. Let $0 < \delta < \frac{1}{2} < \alpha < 1$. Let e, d satisfy $ed \equiv 1 \bmod \phi(N)$, such that bitsize($d$) $= n$ and bitsize(e) $= \alpha n$.
Given the $(1 - \delta)n$ MSBs of d, N can be factored in polynomial time if:

- $\delta \leq \frac{1}{3} + \frac{1}{3}\alpha - \frac{1}{3}\sqrt{4\alpha^2 + 2\alpha - 2} - \epsilon$ *(Section 4.2).*

In Fig. 1 and 2 we illustrate our results on known MSBs of d. In Fig. 1, the fraction of bits required for an attack is plotted as a function of the size of d. It shows the parts of the key space that are insecure by the attacks in Section 4.1, and by the results of [12] and [1]. Fig. 2 is a picture of the relation between the fraction of bits of d required for an attack and the size of e, showing the results of [2], [3], and Section 4.2.

Note that our attacks for known MSBs have natural starting and ending points. One MSB attack on small d coincides with the bound $d \leq N^{0.284}$ from [1], the other runs up to the situation where d is of full size and is fully known. This links our results to that of May [9], proving a deterministic polynomial time equivalence between factoring and full knowledge of d. Our MSB attack on small e is a natural extension of the results of [2] and [3].

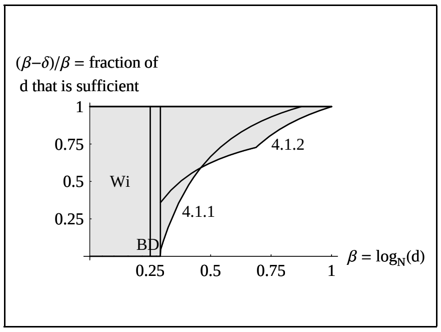

Fig. 1. MSB attacks for small d

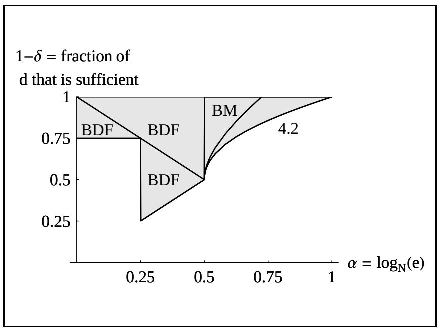

Fig. 2. MSB attacks for small e

Our new result on known LSBs for relatively small d and full size e is as follows.

Theorem 3 (LSB small *d*). *Under a common heuristic assumption concerning resultants, for every $\epsilon > 0$, there exists n_0 such that for every $n > n_0$, the following holds:*
Let $N = pq$ be an n-bit RSA-modulus, and p, q primes of bitsize $\frac{n}{2}$. Let $0 < \delta < \beta < 1$. Furthermore, let e, d satisfy $ed \equiv 1 \bmod \phi(N)$ with bitsize$(e) = n$ and bitsize$(d) = \beta n$. Given the $(\beta - \delta)n$ LSBs of d, N can be factored in polynomial time when:

- $\delta < \frac{5}{6} - \frac{1}{3}\sqrt{1 + 6\beta} - \epsilon$ *(Section 4.3).*

Fig. 3 illustrates our result on known LSBs. The fraction of bits required for an attack is plotted as a function of the size of d. Fig. 4 is a picture of the relation between the fraction of bits required for an attack, and the size of e, showing the work of [2] and [3]. Analysis of our LSB method in the case where e is small results in a bound equivalent to the best result of [3].

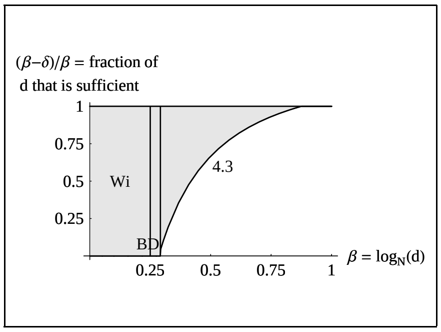

Fig. 3. LSB attacks for small d

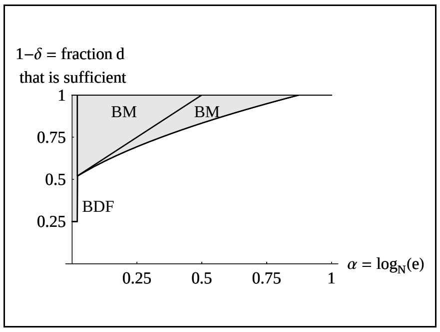

Fig. 4. LSB attacks for small e

Again, notice that the starting point of our new LSB attack for small d coincides with the bound $d \le N^{0.284}$ from [1].

The bounds of Section 4.1.1 and 4.3 show a symmetry in the outcomes of the MSB and LSB situations for small d. Likewise, the bound of Section 4.2 and the second bound of Section 4.1.2 show a symmetry in the outcomes of the MSB cases for small d and small e. This is a result of the general character of our method. Instead of studying only special scenarios, we analyze the underlying polynomials in a general framework, which also makes it possible to study numerous old and new cryptanalytic situations, on which we shall comment in Section 4.4.

Our results can be viewed as evidence that side channel attacks are even more dangerous to RSA than we already knew. In essence, we show that there exist partial key exposure attacks up to full size exponents, hence if either e or d is chosen to be significantly smaller than $\phi(N)$, the system is vulnerable to this type of attacks. This can be understood as a warning to crypto-designers to choose both private and public exponent at random, or take sufficient countermeasures to prevent private key bits from leaking.

This paper is organized as follows. In Section 2, we describe the typical RSA setting and show how we derive polynomials with small roots from the RSA key equation when MSBs or LSBs of the private exponent d are known. In Section 3, we give an overview of the tools we use to find the small roots of these polynomials. In Section 4 we give the description of our attacks, proving the results of Theorem 1, 2, and 3. In Section 5, experimental results are provided.

2 Looking at the RSA Key Equation

Let p, q, N, d, e be as usual, i.e. p and q are distinct primes, $N = pq$ is taken as modulus, and the encryption exponent e and decryption exponent d satisfy $ed \equiv 1 \bmod \phi(N)$. For all of the attacks in this paper, we assume that p and q have the same bitsize, thus $p + q < 3\sqrt{N}$. Let $k \in \mathbb{Z}$ be defined by the RSA key equation

$$ed - 1 = k\phi(N), \quad \text{where } \phi(N) = (p-1)(q-1) = N - (p + q - 1).$$

In our scenario, we assume one of the exponents e and d is chosen to be small and the other one is of full size. We will first focus on the case where d is small. Therefore, we place no restrictions on e except $e < \phi(N)$. It follows that $k < \frac{ed}{\phi(N)} < d$.

When MSBs of d are known, we write $d = \tilde{d} + d_0$, where $\tilde{d}$ (representing the most significant bits of d) is known to the attacker, but d_0 (representing the least significant bits of d) is not. To make this precise, let β and δ be parameters such that $d \le N^{\beta}$, and $|d_0| = |d - \tilde{d}| \le N^{\delta}$.

For the MSB case, we can thus rewrite the RSA key equation into

$$e(\tilde{d} + d_0) - 1 = k(N - (p + q - 1)).$$

Hence, the polynomial

$$f_{MSB1}(x, y, z) = ex - Ny + yz + R, \text{ where } R = e\tilde{d} - 1,$$

has a root $(x_0, y_0, z_0) = (d_0, k, p+q-1)$. Let $X := N^\delta$, $Y := N^\beta$, and $Z := 3N^{\frac{1}{2}}$. Then the root is 'small' since $|x_0| < X$, $|y_0| < Y$, and $|z_0| < Z$.

The attacker can also compute $\tilde{k} = \frac{e\tilde{d}-1}{N}$ as an approximation to k, and set $k_0 = k - \tilde{k}$ as the unknown part of k. It can be shown (as was done in [3]) that $|k_0| < \frac{e}{\phi(N)}(N^\delta + 3N^{\beta-\frac{1}{2}})$, so in our case we have $|k_0| < 4N^\gamma$, where $\gamma = \max\{\delta, \beta - \frac{1}{2}\}$. When we substitute the knowledge of the MSBs of k into the RSA key equation, we obtain

$$e(\tilde{d} + d_0) - 1 = (\tilde{k} + k_0)(N - (p + q - 1)).$$

Hence,

$$f_{MSB2}(x, y, z) = ex - Ny + yz + \tilde{k}z + R, \text{ with } R = e\tilde{d} - 1 - \tilde{k}N,$$

has a root $(x_0, y_0, z_0) = (d_0, k_0, p + q - 1)$. With $X := N^\delta$, $Y := 4N^\gamma$, and $Z := 3N^{\frac{1}{2}}$, we have $|x_0| < X$, $|y_0| < Y$, and $|z_0| < Z$.

When LSBs of d are known, the attacker knows $\bar{d} \equiv d \bmod M$ for some M, and we write $d = \bar{d} + d_1 M$, where $\bar{d}$ and M are known, and d_1 is not. We assume that $d \le N^\beta$, and $d_1 \le N^\delta$. We have no approximation of k in this case, so we rewrite the RSA key equation as

$$e(d_1 M + \bar{d}) - 1 = k(N - (p + q - 1)).$$

Thus,

$$f_{LSB}(x, y, z) = eMx - Ny + yz + R, \text{ with } R = e\bar{d} - 1,$$

has a root $(x_0, y_0, z_0) = (d_1, k, p + q - 1)$. Using $X := N^\delta$, $Y := N^\beta$, and $Z := 3N^{\frac{1}{2}}$, we have $|x_0| < X$, $|y_0| < Y$, and $|z_0| < Z$.

3 Finding Small Roots

We have seen that in several cases, we can obtain d, k and $p+q-1$ when we can find a small root of a certain trivariate polynomial. In this section, we describe some tools that we use to solve this problem of finding small roots. For a polynomial $h(x, y, z) = \sum_{i,j,k} h_{ijk} x^i y^j z^k$, we define $||h(x, y, z)||^2 := \sum_{i,j,k} |h_{ijk}|^2$ and $||h(x, y, z)||_\infty := \max_{i,j,k} |h_{ijk}|$.

In [4], Coppersmith describes rigorous techniques to find small integer roots of polynomials in a single variable modulo n, and of polynomials in two variables over the integers. The methods extend to more variables, making them heuristical. Howgrave-Graham reformulated Coppersmith's ideas of finding modular roots in [6], of which we use the following lemma.

Lemma 1 (Howgrave-Graham). *Let $h(x, y, z) \in \mathbb{Z}[x, y, z]$ be a polynomial which is a sum of at most ω monomials. Suppose that $h(x_0, y_0, z_0) \equiv 0 \bmod n$ for some $|x_0| < X$, $|y_0| < Y$, $|z_0| < Z$, and $||h(xX, yY, zZ)|| < \frac{n}{\sqrt{\omega}}$. Then $h(x_0, y_0, z_0) = 0$ holds over the integers.*

Howgrave-Graham's lemma is usually combined with LLL reduction of lattice bases [7].

Fact 1 (LLL). *Let L be a lattice of dimension ω. In polynomial time, the LLL-algorithm outputs two reduced basis vectors v_1 and v_2, that satisfy*

$$||v_1|| \leq ||v_2|| \leq 2^{\frac{\omega}{4}} \det(L)^{\frac{1}{\omega-1}}.$$

Thus, the condition $2^{\frac{\omega}{4}} \det(L)^{\frac{1}{\omega-1}} < \frac{n}{\sqrt{\omega}}$ implies that polynomials corresponding to the two shortest reduced basis vectors match Howgrave-Graham's bound. This condition reduces to $\det(L) \leq (2^{\frac{-\omega}{4}} \frac{1}{\sqrt{\omega}})^{\omega-1} n^{\omega-1}$. In practice, we ignore terms that do not depend on n, and check only if $\det(L) \leq n^{\omega-1}$.

Coppersmith's technique of finding small roots of polynomials over the integers has so far been less applied in cryptanalysis methods. Recently, Coron [5] reformulated this technique analogous to Howgrave-Graham. Essentially, Coron picks a 'suitable' integer n and transfers the situation into finding a small root modulo n, thereby applying Howgrave-Graham's lemma. In the following sections, we will study the polynomials f_{MSB1}, f_{MSB2}, and f_{LSB} to find their small roots over the integers, analogous to Coron.

4 Description of the Attacks

4.1 Known MSBs and Small d

4.1.1 Attack using f_{MSB1}

We will now describe a method that finds a small root of f_{MSB1} over the integers, and prove the first result of Theorem 1, namely that we have a polynomial time MSB attack when

$$\delta \leq \frac{5}{6} - \frac{1}{3}\sqrt{1+6\beta} - \epsilon.$$

Recalling the situation where we do not use an approximation of k, we want to find a small root (x_0, y_0, z_0) of the polynomial $f_{MSB1}(x, y, z) = ex - Ny + yz + R$.

Our first observation is that f_{MSB1} is irreducible over the integers. Thus, if we could construct two polynomials f_1, f_2 with the same root (x_0, y_0, z_0) which are not multiples of f_{MSB1}, then they do not share a common divisor with f_{MSB1}. Hence, the polynomials $p_1(y, z) = \mathrm{Res}_x(f_{MSB1}, f_1)$ and $p_2(y, z) = \mathrm{Res}_x(f_{MSB1}, f_2)$ cannot be the zero polynomials. Under the heuristic that the resultant $\mathrm{Res}_y(p_1, p_2)$ does not vanish, we obtain $z_0 = p + q - 1$ from a linear factor $(z - z_0)$ in $\mathrm{Res}_y(p_1, p_2)$, which gives us the factorization of N. All attacks in this paper have a similar heuristic concerning resultants, common in cryptanalysis using multivariate polynomials. Therefore we will use the following assumption.

Assumption 1. *The resultant computations for the polynomials in this paper yield non-zero polynomials.*

We will comment on how this assumption holds in practice in Appendix D, where we also provide experimental results.

Now let us find conditions under which we can construct f_1 and f_2 as defined above. Let X, Y, Z be upper bounds for x_0, y_0, z_0, respectively. We fix an integer m depending on $\frac{1}{\epsilon}$, and a parameter t, that we will optimize later in terms of m. We define $W = ||f_{MSB1}(xX, yY, zZ)||_\infty$ and $n = (XY)^m Z^{m+t} W$.

First, in order to work with a polynomial with constant term 1, we define

$$f(x, y, z) \equiv R^{-1} f_{MSB1}(x, y, z) \bmod n \equiv 1 + ax + by + cyz.$$

Let us look at the following collection of polynomials, the so-called shifts:

$$\begin{aligned} g_{ijk}(x, y, z) &= x^i y^j z^k f(x, y, z) X^{m-i} Y^{m-j} Z^{m+t-k}, \\ &\quad \text{for } i = 0, \ldots, m\ ;\ j = 0, \ldots, m-i\ ;\ k = 0, \ldots, j, \\ h_{ijk}(x, y, z) &= x^i y^j z^k f(x, y, z) X^{m-i} Y^{m-j} Z^{m+t-k}, \\ &\quad \text{for } i = 0, \ldots, m\ ;\ j = 0, \ldots, m-i\ ;\ k = j+1, \ldots, j+t. \end{aligned}$$

In addition to the polynomials g and h, we also use the polynomials

$$\begin{aligned} g'_{ijk}(x, y, z) &= n x^i y^j z^k \text{ for } i = 0, \ldots, m+1; j = m+1-i; k = 0, \ldots, j, \\ h'_{ijk}(x, y, z) &= n x^i y^j z^k \text{ for } i = 0, \ldots, m+1; j = m+1-i; k = j+1, \ldots, j+t. \end{aligned}$$

Let us give an intuition of the construction of our collection of polynomials. When $m = t = 1$, the polynomials g are constructed by multiplying f by its monomials 1, x, y, yz and constants. In this way, all the monomials of f^2 appear. In general, the polynomials g are constructed by multiplying f by the monomials of f^m, thereby creating the monomials of f^{m+1}. Additionally, we add the z-shifts h. In our example, the z-shifts are constructed by multiplying f by the terms z, xz, and yz^2 and constants. The terms z, xz, and yz^2 are the multiplications of z and the original monomials, without yz since this shift was already in g. The auxiliary polynomials g', h' contain the monomials in g and h that were not used for shifts.

Obviously, g, h, g', and h' all have the root (x_0, y_0, z_0) modulo n: g and h have f as a factor, and g' and h' are multiples of n. Let f_1 and f_2 be linear combinations of these polynomials. According to Howgrave-Graham's lemma, if $||f_1(xX, yY, zZ)||$ and $||f_2(xX, yY, zZ)||$ are smaller than $\frac{n}{\sqrt{\omega}}$, then f_1 and f_2 both have the root (x_0, y_0, z_0) over the integers.

Moreover, we want to ensure that $f_1(xX, yY, zZ)$ and $f_2(xX, yY, zZ)$ are not multiples of $f_{MSB1}(xX, yY, zZ)$, which implies that f_1, f_2 are not multiples of f. By construction, each of our polynomials $g_{ijk}(xX, yY, zZ)$, $h_{ijk}(xX, yY, zZ)$, $g'_{ijk}(xX, yY, zZ)$, $h'_{ijk}(xX, yY, zZ)$ is divisible by $(XY)^m Z^{m+t}$. So $f_1(xX, yY, zZ)$ and $f_2(xX, yY, zZ)$ must be divisible by this term. According to a lemma of Coron [5, Lemma 3], for any multiple $h(xX, yY, zZ)$ of $f_{MSB1}(xX, yY, zZ)$ it holds that

$$||h(xX, yY, zZ)|| \geq 2^{-(\rho+1)^2} (XY)^m Z^{m+t} \cdot ||f_{MSB1}(xX, yY, zZ)||_\infty = 2^{-(\rho+1)^2} n,$$

where ρ is the maximum degree of the polynomials h and f_{MSB1} in each variable separately. If we let terms that do not depend on n contribute to ϵ, we find that a linear combination with norm smaller than n cannot be a multiple of f_{MSB1}, and must satisfy Howgrave-Graham's bound.

We build a lattice L using as a basis the coefficient vectors of $g_{ijk}(xX, yY, zZ)$, $h_{ijk}(xX, yY, zZ)$, $g'_{ijk}(xX, yY, zZ)$ and $h'_{ijk}(xX, yY, zZ)$. We order the vectors such that the matrix is triangular, and the diagonal entries of g and h are equal to $(XY)^m Z^{m+t}$. For $m = t = 1$, after dividing out XYZ^2 for simplicity, the coefficient matrix is the following (the rows correspond to the coefficient vectors of h, g, h', and g', respectively).

$$
\begin{array}{c}
\begin{array}{cccccccccccccccc}
z & xz & yz^2 & 1 & x & y & yz & x^2z & xyz^2 & y^2z^3 & x^2 & xy & y^2 & y^2z & xyz & y^2z^2 \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow
\end{array} \\
\left(\begin{array}{ccccccc|ccccccccc}
1 & aX & cYZ & & & & bY & & & & & & & & & \\
 & 1 & & & & & & aX & cYZ & & & & & & bY & \\
 & & 1 & & & & & & aX & cYZ & & & & & & bY \\
\hline
 & & & 1 & aX & bY & cYZ & & & & & & & & & \\
 & & & & 1 & & & & & & aX & bY & & & cYZ & \\
 & & & & & 1 & & & & & & aX & bY & cYZ & & \\
 & & & & & & 1 & & & & & & & bY & aX & cYZ \\
\hline
 & & & & & & & WX^2Z & & & & & & & & \\
 & & & & & & & & WXYZ^2 & & & & & & & \\
 & & & & & & & & & WY^2Z^3 & & & & & & \\
\hline
 & & & & & & & & & & WX^2 & & & & & \\
 & & & & & & & & & & & WXY & & & & \\
 & & & & & & & & & & & & WY^2 & & & \\
 & & & & & & & & & & & & & WY^2Z & & \\
 & & & & & & & & & & & & & & WXYZ & \\
 & & & & & & & & & & & & & & & WY^2Z^2
\end{array}\right)
\end{array}
$$

In general, the computations in Appendix A show that for $t = \tau m$, if

$$X^{1+3\tau} Y^{2+3\tau} Z^{1+3\tau+3\tau^2} \leq W^{1+3\tau},$$

we find polynomials f_1 and f_2 that satisfy the Howgrave-Graham bound. Thus, they have the root (x_0, y_0, z_0) over the integers and are not multiples of f. Under Assumption 1, the resultant method will reveal the integer root (x_0, y_0, z_0). Note that the bound can be applied on any irreducible polynomial with the monomials 1, x, y, and yz.

In our case, $X = N^\delta$, $Y = N^\beta$, $Z = 3N^{\frac{1}{2}}$ and $W = \max\{eX, NY, YZ, R\} \geq NY = N^{1+\beta}$. We find an optimal value $\tau = \frac{1}{2} - \delta$, which implies $\delta \leq \frac{5}{6} - \frac{1}{3}\sqrt{1 + 6\beta}$. Thereby, we have derived the first result of Theorem 1.

4.1.2 Attack using f_{MSB2}

We will now show how to obtain the second and third result mentioned in Theorem 1, namely that we have a polynomial time MSB attack whenever

$$\delta \leq \frac{3}{16} - \epsilon \text{ and } \beta \leq \frac{11}{16}, \qquad \text{or} \qquad \delta \leq \frac{1}{3} + \frac{1}{3}\beta - \frac{1}{3}\sqrt{4\beta^2 + 2\beta - 2} - \epsilon \text{ and } \beta \geq \frac{11}{16}.$$

For the situation where we use information on MSBs of d to get an approximation $\tilde{k}$ of k, we want to find a small root (x_0, y_0, z_0) of the polynomial $f_{MSB2}(x, y, z) = ex - Ny + yz + \tilde{k}z + R$.

We fix an integer m depending on $\frac{1}{\epsilon}$, a parameter t that we optimize later, and put $W = ||f_{MSB2}(xX, yY, zZ)||_\infty$, and $n = X^m Y^{m+t} Z^m W$. We compute $f \equiv R^{-1} f_{MSB2} \bmod n \equiv 1 + ax + by + cyz + dz$, and define the collection of polynomials

$$
\begin{aligned}
g_{ijk}(x, y, z) &= x^i y^j z^k f(x, y, z) X^{m-i} Y^{m+t-j} Z^{m-k}, \\
&\quad \text{for } i = 0, \dots, m \ ; \ j = 0, \dots, m - i \ ; \ k = 0, \dots, m - i, \\
h_{ijk}(x, y, z) &= x^i y^j z^k f(x, y, z) X^{m-i} Y^{m+t-j} Z^{m-k}, \\
&\quad \text{for } i = 0, \dots, m \ ; \ j = m - i + 1, \dots, m - i + t \ ; \ k = 0, \dots, m - i, \\
g'_{ijk}(x, y, z) &= n x^i y^j z^k, \\
&\quad \text{for } i = 0, \dots, m + 1 \ ; \ j = 0, \dots, m + t + 1 - i \ ; \ k = m + 1 - i, \\
h'_{ijk}(x, y, z) &= n x^i y^j z^k, \\
&\quad \text{for } i = 0, \dots, m \ ; \ j = m + t + 1 - i \ ; \ k = 0, \dots, m - i.
\end{aligned}
$$

As before, the polynomials g are constructed by shifting f with every monomial of f^m. The polynomials h represent extra y-shifts, the shifts used are y^l times the monomials of f^m, for $l = 1, \dots, t$ (excluding shifts that were already in g). The auxiliary polynomials g' and h' contain the monomials of g and h that were not used for the shifts.

We build a lattice L using as a basis the coefficient vectors of $g_{ijk}(xX, yY, zZ)$, $h_{ijk}(xX, yY, zZ)$, $g'_{ijk}(xX, yY, zZ)$, and $h'_{ijk}(xX, yY, zZ)$, where we order the vectors such that the corresponding lattice basis is triangular, and the diagonal entries of g and h are equal to $X^m Y^{m+t} Z^m$.

The computations in Appendix B show for $t = \tau m$, that when

$$X^{2+3\tau} Y^{3+6\tau+3\tau^2} Z^{3+3\tau} \le W^{2+3\tau}$$

holds, we can find two reduced basis vectors that satisfy the Howgrave-Graham bound. So under Assumption 1, we can find the factorization of N in polynomial time.

In our case, we have $X = N^\delta$, $Y = 4N^\gamma$, with $\gamma = \max\{\delta, \beta - \frac{1}{2}\}$, and $Z = 3N^{\frac{1}{2}}$. Also, $W = \max\{eX, NY, YZ, \tilde{k}Z, R\} \ge NY = 4N^{1+\gamma}$. The optimal value $\tau = \frac{\frac{1}{2} - \delta - \gamma}{2\gamma}$ leads to the condition $\delta \le \frac{1}{3}\gamma + \frac{1}{2} - \frac{1}{3}\sqrt{4\gamma^2 + 6\gamma}$. If $\gamma = \delta$, this implies $\delta \le \frac{3}{16}$, valid for $\beta \le \frac{11}{16}$. If $\gamma = \beta - \frac{1}{2}$, we get $\delta \le \frac{1}{3} + \frac{1}{3}\beta - \frac{1}{3}\sqrt{4\beta^2 + 2\beta - 2}$, valid for $\beta \ge \frac{11}{16}$.

This concludes the proof of Theorem 1.

4.2 Known MSBs and Small e

In practice, one often chooses the public exponent e to be small. Therefore, we now let $e = N^\alpha$ and $d < \phi(N)$. Note that we are able to use the same polynomials f_{MSB1} and f_{MSB2}, when we make some changes in the size of the parameters. The best result in this situation, as mentioned in Theorem 2, is that we obtain a polynomial time MSB attack whenever

$$\delta \le \frac{1}{3} + \frac{1}{3}\alpha - \frac{1}{3}\sqrt{4\alpha^2 + 2\alpha - 2} \ \text{ for } \alpha > \frac{1}{2}.$$

We can again use $f_{MSB1}(x,y,z) = ex - Ny + yz + R$, now with $|d_0| < X = N^{\delta}$, $|k| < Y = N^{\alpha}$ and $|p+q-1| < Z = 3N^{\frac{1}{2}}$. Using $W = N^{1+\alpha}$, as in Section 4.1.1 we find $\delta \leq \frac{5}{6} - \frac{1}{3}\sqrt{1+6\alpha}$. This result only holds for $\alpha > \frac{1}{2}$. In the case $\alpha < \frac{1}{2}$, from [2, Theorem 4.1], we can assume that k is known, and the polynomial to be analyzed becomes bivariate. Since our attack using f_{MSB1} obtains a worse bound than the one using f_{MSB2}, it is not mentioned in Theorem 2.

When we use partial information on k, where k is partly unknown (so $\alpha > \frac{1}{2}$), we can use $f_{MSB2}(x,y,z) = ex - Ny + yz + \tilde{k}z + R$. We have $|d_0| < X = N^{\delta}$, $|k_0| < Y = 4N^{\gamma}$, with $\gamma = \max\{\alpha + \delta - 1, \alpha - \frac{1}{2}\}$, and $|p+q-1| < Z = 3N^{\frac{1}{2}}$. Using $W = N^{1+\gamma}$, we get the same condition as in the previous paragraph, namely $\delta \leq \frac{1}{3}\gamma + \frac{1}{2} - \frac{1}{3}\sqrt{4\gamma^2 + 6\gamma}$, that we analyze for two possibilities for γ.

If we substitute $\gamma = \alpha + \delta - 1$ (in other words, we assume $\delta > \frac{1}{2}$), we obtain the condition $\delta < \frac{3+4\alpha-4\alpha^2}{16\alpha}$. However, for $\alpha > \frac{1}{2}$, $\delta < \frac{3+4\alpha-4\alpha^2}{16\alpha} < \frac{1}{2}$, so we get no result. If $\gamma = \alpha - \frac{1}{2}$, we find $\delta \leq \frac{1}{3} + \frac{1}{3}\alpha - \frac{1}{3}\sqrt{4\alpha^2 + 2\alpha - 2}$. This concludes the proof of Theorem 2.

4.3 Known LSBs and Small d

In this section, we will show how to obtain the result of Theorem 3, namely that we have a polynomial time LSB attack whenever

$$\delta \leq \frac{5}{6} - \frac{1}{3}\sqrt{1+6\beta} - \epsilon.$$

The polynomial $f_{LSB}(x,y,z) = eMx - Ny + yz + R$, where $R = e\bar{d} - 1$, has the same monomials as f_{MSB1}. So we can directly apply the analysis of Section 4.1.1. We use

$$X^{1+3\tau}Y^{2+3\tau}Z^{1+3\tau+3\tau^2} \leq W^{1+3\tau},$$

on $X = N^{\delta}$, $Y = N^{\beta}$, $Z = 3N^{\frac{1}{2}}$ and $W = \max\{eMX, NY, YZ, R\} \geq NY = N^{1+\beta}$. This implies $\delta \leq \frac{5}{6} - \frac{1}{3}\sqrt{1+6\beta}$, which concludes the proof of Theorem 3.

If we adapt the LSB attack for the situation when e is not of full size, we get exactly the result from Blömer and May in [3, Section 6].

4.4 Other Applications of the General Method

We have already mentioned that the analysis of the approaches using f_{MSB1} and f_{MSB2} is general, in the sense that for every irreducible polynomial with the monomials $1, x, y, yz$, the inequality $X^{1+3\tau}Y^{2+3\tau}Z^{1+3\tau+3\tau^2} \leq W^{1+3\tau}$ defines the condition for a successful (heuristic) attack. Also, for every irreducible polynomial with the monomials $1, x, y, yz, z$, the condition $X^{2+3\tau}Y^{3+6\tau+3\tau^2}Z^{3+3\tau} \leq W^{2+3\tau}$ implies a successful (heuristic) attack. As a consequence, many known attacks on RSA are special cases of our general framework.

As could be seen in Fig. 1, and 3, one MSB attack and one LSB attacks for small d coincide with the bound $d < N^{0.284}$ from [1]. This result can also be found using our method by noticing that $f_{BD}(x,y,z) = ex - Ny + yz - 1$ with the root

$(x_0, y_0, z_0) = (d, k, p+q-1)$ has the same monomials as f_{MSB1}. Therefore, we can substitute $X, Y = N^\beta$, $Z = 3N^{\frac{1}{2}}$ and $W = \max\{eX, NY, YZ\} \geq NY = N^{1+\beta}$ in $X^{1+3\tau}Y^{2+3\tau}Z^{1+3\tau+3\tau^2} \leq W^{1+3\tau}$, which leads to $\beta \leq \frac{7}{6} - \frac{1}{3}\sqrt{7} \approx 0.284$. To get the improved Boneh-Durfee bound one has to use sublattices. We leave this for further research.

Fig. 1 also shows that the graph of our (asymptotic) attack of Section 4.1.2 goes up to $\frac{\beta-\delta}{\beta} = 1$, for the parameter choice $\beta = 1$. This links our result to a recent result of May [9], who proves that if one knows all the bits of d and $ed \leq N^2$, then one can factor in deterministic polynomial time.

Moreover, the result on RSA with small prime difference from de Weger [11] and one of the results for unbalanced RSA with small CRT-exponent by May [8] are also special cases of our method, as is an interesting situation not analyzed in the literature before, namely when both some MSBs and some LSBs of the private exponent are known. We will comment on these other applications of our general method in Appendix C.

5 Experiments

We state some experimental results to give an idea of the performance of our methods. In all the cases, $N \approx 2^{1024}$. The experiments are performed on a server containing two Pentium III processors of 1000 Mhz, and all the lattice basis reductions are done using Shoup's NTL [10].

For our MSB1 attack on small d, a typical case is $\beta = 0.3$, $\delta = 0.21$ (e.g. 70% of d is unknown). An attack using $m = 2$, $t = 1$ involved a 10 minute reduction of the 30-dimensional lattice.

For the MSB2 attack on small d, a typical case is $\beta = 0.6$, $\delta = 0.13$ (e.g. 22% of d is unknown). The attack using $m = 2$, $t = 2$ has a 50-dimensional lattice, that took $3\frac{1}{4}$ hours to reduce.

We performed the MSB2 attack on small e for $\alpha = 0.7$, $\delta = 0.08$ (e.g. 8% of d is unknown), using $m = 2$, $t = 2$. The reduction of the 50-dimensional lattice took $2\frac{3}{4}$ hours.

All typical cases are examples of our attacks where the bound on δ that we obtain in practice (for the low value $m = 2$) already exceeds the asymptotic bounds of other known attacks. More experimental results are included in Appendix D, where we also comment on how Assumption 1 holds in practice.

Last of all, we want to note that one could also apply the original method of Coppersmith described in [4] instead of Coron's reformulation [5]. In that case, the formulation of the method is a bit more technical, and the method produces essentially the same asymptotic bounds, but it has the advantage that the dimension of the lattice to reduce drops from a cubic to a quadratic function in m, which could significantly reduce the time necessary for LLL reduction.

References

1. Dan Boneh and Glenn Durfee: Cryptanalysis of RSA with Private Key d Less Than $N^{0.292}$, IEEE Transactions on Information Theory **46** [2000], 1339–1349.
2. Dan Boneh, Glenn Durfee and Yair Frankel: An Attack on RSA given a Small Fraction of the Private Key Bits, Proceedings of ASIACRYPT 1998, LNCS **1514** [1998], 25–34.
3. Johannes Blömer and Alexander May: New Partial Key Exposure Attacks on RSA, Proceedings of CRYPTO 2003, LNCS **2729** [2003], 27–43.
4. Don Coppersmith: Small Solutions to Polynomial Equations and Low Exponent RSA Vulnerabilities, Journal of Cryptology **10** [1997], 233–260.
5. Jean-Sébastien Coron: Finding Small Roots of Bivariate Integer Equations Revisited, Proceedings of EUROCRYPT 2004, LNCS **3027** [2004], 492–505.
6. Nick Howgrave-Graham: Finding Small Roots of Univariate Modular Equations Revisited, Cryptography and Coding, LNCS **1355** [1997], 131–142.
7. Arjen Lenstra, Hendrik Lenstra, Jr., and László Lovász: Factoring Polynomials with Rational Coefficients, Mathematische Ann. **261** [1982], 513–534.
8. Alexander May: Cryptanalysis of Unbalanced RSA with Small CRT-Exponent, Proceedings of CRYPTO 2002, LNCS **2442** [2002], 242–256.
9. Alexander May: Computing the RSA Secret Key is Deterministic Polynomial Time Equivalent to Factoring, Proceedings of CRYPTO 2004, LNCS **3152** [2004], 213–219.
10. Victor Shoup: NTL: A Library for doing Number Theory, online available at http://shoup.net/ntl
11. Benne de Weger: Cryptanalysis of RSA with Small Prime Difference, Applicable Algebra in Engineering, Communication and Computing **13** [2002], 17–28.
12. Michael Wiener: Cryptanalysis of Short RSA Secret Exponents, IEEE Transactions on Information Theory **36** [1990], 553–558.

A The bound $X^{1+3\tau}Y^{2+3\tau}Z^{1+3\tau+3\tau^2} \le W^{1+3\tau}$

In this appendix, we show how to obtain the bound $X^{1+3\tau}Y^{2+3\tau}Z^{1+3\tau+3\tau^2} \le W^{1+3\tau}$ for the attack using f_{MSB1} (Section 4.1.1).

In Section 4.1.1, we described how to construct the lattice. The matrix containing the basis vectors is triangular and has the following diagonal entries (corresponding to the polynomials g, h, g' and h', respectively):

$$
\begin{array}{ll}
X^mY^mZ^{m+t} & \text{for } i=0,\ldots,m; j=0,\ldots,m-i; k=0,\ldots,j \\
X^mY^mZ^{m+t} & \text{for } i=0,\ldots,m; j=0,\ldots,m-i; k=j+1,\ldots,j+t \\
X^{m+i}Y^{m+j}Z^{m+t+k}W & \text{for } i=0,\ldots,m+1; j=m+1-i; k=0,\ldots,j \\
X^{m+i}Y^{m+j}Z^{m+t+k}W & \text{for } i=0,\ldots,m+1; j=m+1-i; k=j+1,\ldots,j+t
\end{array}
$$

Since we have to optimize t in terms of m, we put $t=\tau m$. Elementary computations show that the dimension of L is

$$\omega = \frac{1}{6}(m^3(1+3\tau)+m^2(9+15\tau)) + o(m^2),$$

and that

$$\begin{aligned}\det(L) = & X^{\frac{1}{6}(m^4(1+3\tau)+m^3(10+18\tau)+o(m^3))} \cdot Y^{\frac{1}{6}(m^4(1+3\tau)+m^3(11+18\tau)+o(m^3))} \\ & \cdot Z^{\frac{1}{6}(m^4(1+4\tau+3\tau^2)+m^3(10+27\tau+18\tau^2)+o(m^3))} \cdot W^{\frac{1}{6}(m^2(3+6\tau)+o(m^2))}.\end{aligned}$$

When we apply LLL-reduction to our lattice, the polynomials $f_1(x,y,z)$ and $f_2(x,y,z)$ corresponding to the shortest two vectors in the reduced basis satisfy $f_1(x_0,y_0,z_0) \equiv 0 \bmod n$ and $f_2(x_0,y_0,z_0) \equiv 0 \bmod n$. In order to apply Howgrave-Graham's lemma, we explained in Section 3 that

$$\det(L) \leq (2^{\frac{-\omega}{4}} \frac{1}{\sqrt{\omega}})^{\omega-1} n^{\omega-1}.$$

must hold.

Ignoring terms that do not depend on $n = X^m Y^m Z^{m+t} W$, and ignoring terms of order $o(m^3)$ (we let these terms contribute to ϵ), we obtain that if

$$X^{m^4(1+3\tau)+m^3(10+18\tau)} Y^{m^4(1+3\tau)+m^3(11+18\tau)} Z^{m^4(1+4\tau+3\tau^2)+m^3(10+27\tau+18\tau^2)} \leq (XYZ^{1+\tau})^{m^4(1+3\tau)+m^3(9+15\tau)} W^{m^3(1+3\tau)}$$

the polynomials $f_1(x,y,z)$ and $f_2(x,y,z)$ satisfy the Howgrave-Graham bound. The condition above simplifies into

$$X^{1+3\tau} Y^{2+3\tau} Z^{1+3\tau+3\tau^2} \leq W^{1+3\tau}.$$

B The bound $X^{2+3\tau} Y^{3+6\tau+3\tau^2} Z^{3+3\tau} \leq W^{2+3\tau}$

In this appendix, we show how to obtain the bound $X^{2+3\tau} Y^{3+6\tau+3\tau^2} Z^{3+3\tau} \leq W^{2+3\tau}$ for the attack using f_{MSB2} (Section 4.1.2).

In Section 4.1.2, we described how to construct the lattice. The matrix containing the basis vectors is triangular and has the following diagonal entries (corresponding to g, h, g', and h'):

$X^m Y^{m+t} Z^m$	for $i = 0,\ldots,m; j = 0,\ldots,m-i; k = 0,\ldots,m-i$
$X^m Y^{m+t} Z^m$	for $i = 0,\ldots,m; j = m-i+1,\ldots,m-i+t;$ $k = 0,\ldots,m-i$
$X^{m+i} Y^{m+t+j} Z^{m+k} W$	for $i = 0,\ldots,m+1; j = 0,\ldots,m+t+1-i;$ $k = m+1-i$
$X^{m+i} Y^{m+t+j} Z^{m+k} W$	for $i = 0,\ldots,m; j = m+t+1-i; k = 0,\ldots,m-i$

One can check that

$$\dim(L) = \omega = \frac{1}{6}(m^3(2+3\tau) + m^2(15+15\tau)) + o(m^2),$$

and the determinant of L is equal to

$$\begin{aligned}& X^{\frac{1}{6}(m^4(2+3\tau)+m^3(17+18\tau)+o(m^3))} \cdot Y^{\frac{1}{6}(m^4(2+5\tau+3\tau^2)+m^3(18+36\tau+18\tau^2)+o(m^3))} \\ & \cdot Z^{\frac{1}{6}(m^4(2+3\tau)+m^3(18+18\tau)+o(m^3))} \cdot W^{\frac{1}{6}(m^2(6+6\tau)+o(m^2))}.\end{aligned}$$

When we apply LLL-reduction to our lattice, the polynomials $f_1(x,y,z)$ and $f_2(x,y,z)$ corresponding to the shortest two vectors in the reduced basis satisfy $f_1(x_0,y_0,z_0) \equiv 0 \bmod n$ and $f_2(x_0,y_0,z_0) \equiv 0 \bmod n$. In order to apply Howgrave-Graham's Lemma, it must hold that

$$\det(L) \leq (2^{\frac{-\omega}{4}} \frac{1}{\sqrt{\omega}})^{\omega-1} n^{\omega-1}.$$

Ignoring terms that do not depend on $n = X^m Y^{m+t} Z^m W$, and ignoring terms of order $o(m^3)$ (we let these terms contribute to ϵ), we obtain that if

$$X^{m^4(2+3\tau)+m^3(17+18\tau)} Y^{m^4(2+5\tau+3\tau^2)+m^3(18+36\tau+18\tau^2)} Z^{m^4(2+3\tau)+m^3(18+18\tau)} \leq (XY^{1+\tau}Z)^{m^4(2+3\tau)+m^3(15+15\tau)} W^{m^3(2+3\tau)}$$

the polynomials $f_1(x,y,z)$ and $f_2(x,y,z)$ satisfy Howgrave-Graham's bound. The condition above simplifies into

$$X^{2+3\tau} Y^{3+6\tau+3\tau^2} Z^{3+3\tau} \leq W^{2+3\tau}.$$

C Other Special Cases of our Method

In this appendix, we show that results from [11] and [8] are also special cases of our method, as is the case where both MSBs and LSBs of d are known.

In the case of RSA with small prime difference, described by de Weger in [11], we have $p - q \leq N^{\beta}$, $k \leq d \leq N^{\delta}$ and $p + q - 2\sqrt{N} \leq N^{2\beta-\frac{1}{2}}$. The function $f_{dW}(x,y,z) = ex - y(N - 2\sqrt{N} - z) - 1$ has the same monomials as f_{MSB1}. When we substitute $X, Y = N^{\delta}$, $Z = N^{2\beta-\frac{1}{2}}$, we find that for $\beta < \frac{3}{4}$, we have $W = N^{1+\delta}$. Using $X^{1+3\tau} Y^{2+3\tau} Z^{1+3\tau+3\tau^2} \leq W^{1+3\tau}$, we get $\delta \leq \frac{1}{6}(4\beta + 5) - \frac{1}{3}\sqrt{(4\beta+5)(4\beta-1)}$. To obtain de Weger's second bound, sublattices are needed.

Also, a bound for unbalanced RSA with small CRT-exponent by May [8] can be derived from our inequality belonging to f_{MSB1}. The setting is $ed_p - k(p - 1) - 1 = 0$, where $d_p \leq N^{\delta}$, $p \geq N^{1-\beta}$, and $k \leq N^{\beta+\delta}$. Multiplication with q yields $ed_p q - (k-1)(N - q) - N = 0$. This gives us the polynomial $f_{Ma1} = ex - y(N - z) - N$. The upper bounds for the root $(x_0, y_0, z_0) = (d_p q, k - 1, q)$ are $X, Y = N^{\beta+\delta}$ and $Z = N^{\beta}$. Additionally, we have $W = N^{1+\beta+\delta}$. Plugging these values in our inequality, we find the bound $\delta \leq 1 - \frac{2}{3}(\beta + \sqrt{3\beta + \beta^2})$.

The last special case we describe in this appendix is the the situation where both MSBs and LSBs of an exponent d are known. Let d_L be a known LSB part of size N^{κ} of the key d, followed by an unknown middle part x of size N^{δ}, which itself is followed by a known MSB part d_M, of size $N^{\beta-\kappa-\delta}$. Hence, we can write d as $d = d_L + M_1(x + M_2 d_M)$, where $M_1 \geq N^{\kappa}$, and $M_2 \leq N^{\delta}$. Note that $\kappa = 0$ describes the case where only MSBs are known, whereas $\kappa = \beta - \delta$ corresponds to the LSB scenario.

When we omit partial knowledge of k, the function $f_{MSB+LSB1}(x,y,z) = eM_1 x - Ny + yz + R$, with $R = ed_L + eM_1 M_2 d_M - 1$, has the small root $(x_0, y_0, z_0) = (x, k, p + q - 1)$, with $X = N^{\delta}$, $Y = N^{\beta}$, and $Z = 3N^{\frac{1}{2}}$.

As the function has the same monomials as f_{MSB1}, one can use the same inequality to conclude that the attack works for $\delta < \frac{5}{6} - \frac{1}{3}\sqrt{1+6\beta}$. Hence, the result is exactly the same as when only MSBs or only LSBs are known and knowledge of k is not used. Apparently, as long as the unknown part of d is connected, its place does not make a difference, only its length.

When we use the partial knowledge of k provided by the approximation $\tilde{k}$, we obtain the function $f_{MSB+LSB2}(x, y, z) = eM_1x - Ny + yz + \tilde{k}z + R$, with $R = ed_L + eM_1M_2d_M - \tilde{k}N - 1$.

Analysis similar to the f_{MSB2} case shows that if $\gamma = \max\{\delta + \kappa, \beta - \frac{1}{2}\} = \delta + \kappa$, we obtain the bound $\delta \leq \frac{3-4\kappa-4\kappa^2}{16+16\kappa}$, valid for $\beta \leq \frac{11+4\kappa-4\kappa^2}{16+16\kappa}$. In the case $\gamma = \beta - \frac{1}{2}$, we find that the attack works whenever $\delta \leq \frac{1}{3} + \frac{1}{3}\beta - \frac{1}{3}\sqrt{4\beta^2 + 2\beta - 2}$, valid for $\beta \geq \frac{11+4\kappa-4\kappa^2}{16+16\kappa}$.

Naturally, equivalent bounds can be derived when d is full size and e is not.

D More Experimental Results

In addition to Section 5, we now show more experimental results. The experiments we did for this appendix are only for $m = 1$ and $m = 2$, which means the lattices are relatively small and the lattice reduction can be performed in a matter of seconds or minutes. In the full version of this paper, experiments for larger parameters will be included.

As in Section 5, the experiments are performed on a server containing two Pentium III processors of 1000 Mhz, and all the lattice basis reductions are done using Shoup's NTL [10]. In contrast to the experimental results mentioned in Section 5, we assume here that we have a 256 bit modulus. So one has to keep in mind that for $N \approx 2^{1024}$, the running time of the LLL-procedure will be longer.

As the bounds on δ stated in Theorem 1 and 2 are asymptotic bounds, the goal of the tables in this appendix is to provide some intuition of what bounds on δ our attacks can achieve in practice. For example, the table in Fig. 5 shows that for $\beta = 0.3$, the asymptotic bound of the attack using f_{MSB1} from Section 4.1.1 is $\delta < 0.28 - \epsilon$. When we use the parameters $m = 2$, $t = 1$, our attack works for $\delta < 0.21$. The attack involves a lattice of dimension 30, which takes approximately 25 seconds to reduce.

This example is one of the three so-called 'typical cases' of Section 5. These are examples where the bound on δ that we obtain in practice exceeds the asymptotic bounds of other known attacks. In the tables in this appendix, the typical cases are written in bold.

For the choice of t, recall from Section 4.1.1 that $t = \tau m$, and that we use $\tau = \frac{1}{2} - \delta$ to obtain the asymptotic result of our attack using f_{MSB1}. This explains that for $m = 1$ in Fig. 5, a value of t larger than 1 gives no significant improvement, but for $m = 2$, $t = 2$ may give a better result when the bound on δ is 'low'. For the attacks using f_{MSB2} (Section 4.1.2 and 4.2), $\tau = \frac{\frac{1}{2}-\delta-\gamma}{2\gamma}$. This explains for example, that when $e = N^\alpha$ with α close to $\frac{1}{2}$, using a larger t gives a better bound on δ in the experiments (as can be seen in Fig. 7).

β	δ	$m = 1$			$m = 2$		
	asympt.	$t = 0$	$t = 1$	$t = 2$	$t = 0$	$t = 1$	$t = 2$
0.30	**0.28**	0.19	0.19	0.19	0.19	**0.21**	0.21
0.35	0.25	0.13	0.14	0.14	0.14	0.16	0.16
0.40	0.22	0.09	0.11	0.11	0.09	0.14	0.15
0.45	0.19	0.04	0.10	0.10	0.05	0.12	0.12
0.50	0.17	0	0.08	0.09	0	0.10	0.11
0.55	0.14	0	0.08	0.08	0	0.09	0.11
0.60	0.12	0	0.04	0.04	0	0.06	0.10
0.65	0.10	0	0	0	0	0	0.06
0.70	0.07	0	0	0	0	0	0.01
0.75	0.05	0	0	0	0	0	0
0.80	0.03	0	0	0	0	0	0
0.85	0.01	0	0	0	0	0	0
Dimension:		10	16	22	20	**30**	40
LLL (sec):		1	2	8	3	**25**	100

Fig. 5. Experiments f_{MSB1} for small d

β	δ	$m = 1$				$m = 2$		
	asympt.	$t = 0$	$t = 1$	$t = 2$	$t = 3$	$t = 0$	$t = 1$	$t = 2$
0.30	0.19	0.19	0.20	0.20	0.20	0.19	0.19	0.19
0.35	0.19	0.15	0.16	0.16	0.16	0.16	0.16	0.16
0.40	0.19	0.12	0.12	0.12	0.12	0.14	0.15	0.15
0.45	0.19	0.10	0.11	0.12	0.12	0.12	0.13	0.13
0.50	0.19	0.08	0.11	0.12	0.12	0.12	0.13	0.13
0.55	0.19	0.08	0.11	0.12	0.12	0.11	0.13	0.13
0.60	**0.19**	0.05	0.11	0.11	0.11	0.11	0.12	**0.13**
0.65	0.19	0	0.05	0.06	0.06	0.05	0.08	0.10
0.70	0.18	0	0	0	0	0	0.04	0.05
0.75	0.14	0	0	0	0	0	0	0
0.80	0.11	0	0	0	0	0	0	0
0.85	0.08	0	0	0	0	0	0	0
0.90	0.05	0	0	0	0	0	0	0
0.95	0.03	0	0	0	0	0	0	0
Dimension:		14	20	26	32	30	40	**50**
LLL (sec):		1	7	17	40	26	180	**480**

Fig. 6. Experiments f_{MSB2} for small d

α	δ	$m = 1$				$m = 2$		
	asymptotic	$t = 0$	$t = 1$	$t = 2$	$t = 3$	$t = 0$	$t = 1$	$t = 2$
0.50	0.50	0.25	0.33	0.38	0.40	0.32	0.37	0.41
0.55	0.33	0.17	0.21	0.23	0.25	0.21	0.23	0.24
0.60	0.27	0.09	0.14	0.17	0.18	0.13	0.16	0.19
0.65	0.22	0.02	0.07	0.10	0.10	0.07	0.11	0.13
0.70	0.18	0	0.02	0.03	0.04	0.02	0.04	**0.08**
0.75	0.14	0	0	0	0	0	0.01	0.02
0.80	0.11	0	0	0	0	0	0	0
0.85	0.08	0	0	0	0	0	0	0
0.90	0.05	0	0	0	0	0	0	0
0.95	0.03	0	0	0	0	0	0	0
Dimension:		14	20	26	32	30	40	**50**
LLL (sec):		1	5	13	40	33	180	**520**

Fig. 7. Experiments f_{MSB2} for small e

Having done some experiments, we can now comment on Assumption 1. Let $g(x, y, z)$ and $h(x, y, z)$ be polynomials that correspond to LLL-reduced vectors in our method, for which Howgrave-Graham's bound is satisfied. If $g(x_0, y_0, z_0) = h(x_0, y_0, z_0) = 0$, but the resultant computations with g and h yield the zero-polynomial, then Assumption 1 does not hold. Therefore, we performed some tests to see how often this occurs. We found that for approximately 0.1% of pairs (g, h) the heuristic failed. This does not mean that the method will always fail in these cases. Usually, there are several vectors that satisfy Howgrave-Graham's bound, hence if one pair fails, other pairs can yield the solution.

Experiments also show that the theoretical bound under which our methods works, $\det(L) \leq (2^{\frac{-\omega}{4}} \frac{1}{\sqrt{\omega}})^{\omega-1} n^{\omega-1}$, is far too strict. It would imply that for $m \in \{1, 2\}$, the method will never work, which clearly contradicts the practice. This is both due to the term $(2^{\frac{-\omega}{4}} \frac{1}{\sqrt{\omega}})^{\omega-1}$, when it is known that LLL-reduction achieves much better bounds in practice, and to the fact that we use the LLL-bound for the second smallest reduced vector. In practice, we experienced that our method works until we come close to $\det(L) \leq n^{\omega}$ (the bound for the first reduced vector to be small enough, omitting the constant term).