New Partial Key Exposure Attacks on RSA Revisited

M. Jason Hinek
School of Computer Science, University of Waterloo
Waterloo, Ontario, N2L-3G1, Canada
mjhinek@alumni.uwaterloo.ca

March 17, 2004

Abstract

At CRYPTO 2003, Blömer and May presented new partial key exposure attacks against RSA. These were the first known polynomial-time partial key exposure attacks against RSA with public exponent $e > N^{1/2}$. Attacks for known most significant bits and known least significant bits were presented.

In this work, we extend their attacks to multi-prime RSA. For r-prime RSA, these result in the first known partial key attacks for public exponent $e > N^{1/r}$. As with other attacks on RSA that have been extended to multi-prime RSA, we show that these attacks are weakened with each additional prime added to the RSA modulus. Some experimental bounds on the fraction of bits needed to mount the attacks are presented for some common RSA modulus sizes and small lattice dimensions.

When using Coppersmith's method for finding small roots of multivariate modular polynomials in cryptographic applications, it is often heuristically assumed that the polynomials resulting from the lattice basis reduction are algebraically independent. For some of Blömer and May's attacks we have observed that this is not the case. Interestingly, even when the polynomials are algebraically dependent in these attacks we are still able to recover the private exponent by simply removing the common factors of the polynomials before computing any resultants.

1 Introduction

A partial key exposure attack is an attack that uses some knowledge of the private key to fully reconstruct it. For RSA (and multi-prime RSA) the private key consists of the modulus N and private (decryption) exponent d. Since N is publicly known, a partial key exposure attack on RSA (and multi-prime RSA) is one in which an adversary uses some of the bits of d to try to reconstruct all of d. While there are no restrictions on which bits of d are known, of particular

interest are attacks which use some number of either the most significant bits or least significant bits. This is because it has been shown that side channel attacks can actually allow an adversary to obtain some number of the most or least significant bits of the private key.

In 1998, Boneh, Durfee, and Frankel [4] presented the first known polynomial-time partial key exposure attacks on RSA. Attacks using both known least significant bits and known most significant bits were presented. All of the attacks were against RSA with public exponent $e < N^{1/2}$. Whether attacks existed for public exponent $e > N^{1/2}$ was left as an open problem.

At CRYPTO 2003, this open problem was answered by Blömer and May who presented polynomial-time partial key exposure attacks on RSA with public exponent $e > N^{1/2}$. Attacks with known least significant bits and known most significant bits were presented as well as attacks with partial knowledge of $d_p \equiv d \pmod{p}$ where p is one of the prime divisors of the modulus.

The goal of this work is to extend these new partial key attacks to multi-prime RSA. We will show that all three attacks presented by Blömer and May can be extended to multi-prime RSA. As with other attacks on RSA that have been extended to multi-prime RSA [9], we find that the attacks become weaker with each additional prime in the modulus.

The rest of this work is organized as follows: the remainder of this section introduces some notation and assumptions concerning multi-prime RSA and reviews Coppersmith's method for finding small solutions of modular multivariate polynomials. In Sections 2-4 we present the attacks giving both asymptotic and experimental results. Section 2 extends Blömer and May's partial key exposure attack with known most significant bits. Sections 3 and 4 extend their partial key exposure attacks with known least significant bits known to multi-prime RSA. The first is a provable attack for small public exponent ($e < N^{1/r}$). The second is heuristic but work for public exponents $e > N^{1/r}$. Finally, in Section 5, we conclude by comparing the security of RSA versus multi-prime RSA with respect to all known partial key exposure attacks.

1.1 Multi-prime RSA

We begin by describing a simplified (or textbook) version multi-prime RSA. For any integer $r \geq 2$, r-prime RSA consists of the following three algorithms:

Key Generation: Let N be the product of r randomly chosen distinct primes $p_1, \ldots, p_r$. Compute Euler's totient function of N : $\phi(N) = \prod_{i=1}^{r}(p_i - 1)$. Choose an integer e, $1 < e < \phi(N)$, such that $\gcd(e, \phi(N)) = 1$. The pair (N, e) is the public key. Compute the unique $d \in \mathbb{Z}_N$ such that $ed \equiv 1 \bmod \phi(N)$ (i.e., compute $d = e^{-1} \bmod \phi(N)$). The private key is the pair (N, d).

Encryption: For any message $m \in \mathbb{Z}_N$, the ciphertext is computed as $c = m^e \bmod N$.

Decryption: For any ciphertext $c \in \mathbb{Z}_N$, the plaintext is recovered by computing $m = c^d \bmod N$.

We call N the multi-prime RSA modulus, the RSA modulus (when $r = 2$), or simply the modulus. The integer e is called the public (or encrypting) exponent and d is called the private (or decrypting) exponent.

When $r = 2$ we have the original RSA encryption scheme. Superficially, the only difference between RSA and multi-prime RSA with $r > 2$ is the number of primes in the modulus. There are practical reasons for using more primes in the modulus however, which can be found in the implementation details of the decryption algorithm. The first advantage is time; using the Chinese Remainder Theorem and performing calculations in parallel, the number of bit operations needed to decrypt a ciphertext is at most $\frac{3}{2r^3}(\log_2 N)^3$. So, the time needed for decryption decreases with each additional prime in the modulus. The second advantage is space; again, using the Chinese Remainder Theorem the space needed for all decryption computations until the very last (recombining step) require only $\log_2 p_r$ space, where p_r is the largest prime in the modulus. If all the primes are roughly $(\log_2 N)/r$-bits large (balanced primes), the space required decreases with each additional prime added to the modulus. Of course, using too many primes increases the risk of the modulus being factored. Since the size of the smallest prime in the modulus is at most $(\log_2 N)/r$-bits long, the modulus is at more of a risk of being factored with the elliptic curve method for factoring with each additional prime. The maximum number of primes that is considered safe for any size modulus is usually taken to be the largest value of r such that using the elliptic curve method is not faster than using the number field sieve to factor N. In these estimates, it is assumed that balanced primes are used. That is, each prime in the modulus is roughly the same size ($(\log_2 N)/r$-bits). This maximizes the size of the smallest prime and so maximizes the estimated runtime of the elliptic curve method. See Lenstra [11] for more detail on choosing a safe number of primes.

We now give some notation and assumptions used in the rest of this work. First, we only consider r-prime RSA with balanced primes. We label the primes so that $p_i < p_{i+1}$ for $i = 1, \ldots, r-1$, and assume that

$$4 < \frac{1}{2}N^{1/r} < p_1 < N^{1/r} < p_r < 2N^{1/r}. \tag{1}$$

The modulus is given by $N = \prod_{i=1}^{r} p_i$ and Euler's totient function for N is simply $\phi(N) = \prod_{i=1}^{r}(p_i - 1)$. The equivalence relation $ed \equiv 1 \bmod \phi(N)$ is called the the public/private key relation. Writing this relation as an equation yields

$$ed - k\phi(N) = 1,$$

where k is some positive integer. We call this equation the public/private key equation. It is often convenient to express $\phi(N)$ in terms of the modulus: $\phi(N) = N - \Lambda$. Defining the set $S_r = \{1, \ldots, r\}$ we see that Λ can be ex-

pressed as

$$\Lambda = N - \phi(N) = \sum_{i \in S_r} N/p_i - \sum_{\substack{i,j \in S_r \\ i \neq j}} N/(p_i p_j) + \cdots + (-1)^r.$$

A simple computation using the above expression for Λ and (1) shows that Λ satisfies

$$\Lambda = N - \phi(N) < (2r-1)N^{1-1/r}.$$

Another convenient way of writing $\phi(N)$ is as a fraction of the modulus: $\phi(N) = N^{1-\lambda}$, where λ is a small number. Some approximate sizes of λ for different modulus sizes for the first few values of r are shown in Table 1.

	Size of modulus (bits)		
r	1024	2048	4096
2	10^{-154}	10^{-308}	10^{-616}
3	10^{-102}	10^{-205}	10^{-411}
4		10^{-154}	10^{-308}
5			10^{-246}

TABLE 1: Approximate size of λ for different modulus sizes for the first few values of r.

The public and private exponents will often be expressed as a fraction of the modulus. We use α to denote the size of the public exponent ($e = N^\alpha$), and δ to denote the size of the private exponent ($d = N^\delta$). The private exponent is always considered to be a $(\log_2 N)$-bit number. If $\log_2 d < \log_2 N$, we simply assume there are leading zeroes in its representation. This allows us express a given number of most significant or least significant bits as a fraction of N, independent of the size of d.

Also, we often use MSB and LSB as shorthand for most significant bits and least significant bits, respectively.

1.2 Coppersmith's Method

We briefly review a method of finding small roots of modular multivariate polynomials. The method is based on Coppersmith's method for finding small roots of bivariate polynomials over $\mathbb{Z}$ [6, 7, 8] as simplified by Howgrave-Graham [10].

Consider a multivariate polynomial $f \in \mathbb{Z}[x_1, \ldots, x_\eta]$ that has a small root $\hat{\mathbf{x}} = (\hat{x}_1, \ldots, \hat{x}_\eta)$ modulo M. That is, $f(\hat{\mathbf{x}}) \equiv 0 \bmod M$. Let $X_1, \ldots, X_\eta$ be defined such that $\hat{x}_1 \leq X_1, \ldots, \hat{x}_\eta \leq X_\eta$.

For some fixed parameter m (a positive integer), new polynomials are constructed of the form

$$f_{\gamma_1,\ldots,\gamma_\eta,j} = x_1^{\gamma_1} \cdots x_\eta^{\gamma_\eta} \cdot M^j \cdot f^{m-j}, \tag{2}$$

where $j \leq m$ and all the γ_i are non-negative integers. By construction, $\hat{\mathbf{x}}$ is a root of $f_{\gamma_1,\ldots,\gamma_\eta,j}$ modulo M^m. Also, for any fixed j, all polynomials of the form (2) with different $(\gamma_1,\ldots,\gamma_\eta)$ values are linearly independent. Using the coefficient vectors of

$$f_{\gamma_1,\ldots,\gamma_\eta,j}(x_1X_1,\ldots,x_\eta X_\eta)$$

for $n \geq \eta$ such linearly independent polynomials, a basis B for a lattice L is constructed (the coefficient vector for each polynomial is used as a basis vector). Each vector in the lattice L will then correspond to a polynomial that has $\hat{\mathbf{x}}$ as a root modulo M^m. A vector $\ell \in L$ corresponds to a polynomial $p \in \mathbb{Z}[x_1,\ldots,x_\eta]$ if and only if the coefficient vector of $p(x_1X_1,\ldots,x_\eta X_\eta) = \ell$.

With a clever choice of the $(\gamma_1,\ldots,\gamma_\eta,j)$ one can construct B so that the lattice is full rank (n) and the basis matrix is triangular. Having a triangular matrix basis is important to allow easy computation of the lattice determinant (volume).

Using Lenstra, Lenstra, and Lovász's [12] lattice basis reduction algorithm, we can then find η vectors in the lattice L with small norms. These new, small normed, vectors are simply the basis vectors of the reduced basis. The following result by Proos [14] gives bounds on the size of these vectors.

Theorem 1 (LLL-Reduced Bases). *Let $L \in \mathbb{Z}^n$ be a lattice spanned by $\{v_1,\ldots,v_n\}$. With $\{v_1,\ldots,v_n\}$ as input the L^3-algorithm outputs in polynomial time a reduced lattice basis $\{v'_1,\ldots,v'_n\}$ for L such that*

$$\|v'_\ell\| \leq 2^{\frac{n+\ell-2}{4}} \det(L)^{\frac{1}{n-\ell+1}} \tag{3}$$

for $\ell = 1$ or any $1 < \ell \leq n$ provided $\|v'_1\| \geq 2^{\frac{\ell-2}{4}}$.

The condition that $\|v'_1\| \geq 2^{\frac{\ell-2}{4}}$ is easily satisfied for the lattices considered here. We then apply a result of Howgrave-Graham to the polynomials whose coefficient vectors are the η small vectors obtained from the LLL-algorithm.

Theorem 2 (Howgrave-Graham). *Let $f(x_1,\ldots,x_\eta)$ be a polynomial that is the sum of at most n monomials and M be a positive integer. Suppose that*

1. *$f(\hat{x}_1,\ldots,\hat{x}_\eta) \equiv 0 \bmod M$, where $|\hat{x}_1| \leq X_1,\ldots,|\hat{x}_\eta| \leq X_\eta$,*
2. *$\|f(x_1X_1,\ldots,x_\eta X_\eta)\| < \frac{M}{\sqrt{n}}$.*

Then $f(\hat{x}_1,\ldots,\hat{x}_\eta) = 0$ holds over the integers.

Proof. Let $f(x_1,\ldots,x_\eta) = \sum_{i=1}^{n} \left(a_i \prod_{j=1}^{\eta} x_j^{e_j}\right)$, where each $e_j \in \mathbb{Z}$ is non-negative. Then,

$$\begin{aligned}
|f(\hat{x}_1,\ldots,\hat{x}_\eta)| &\leq \sum_{i=1}^{n} \left| a_i \prod_{j=1}^{\eta} x_j^{e_j} \right| \leq \sum_{i=1}^{n} \left| a_i \prod_{j=1}^{\eta} X_j^{e_j} \left(\frac{x_j^{e_j}}{X_j^{e_j}}\right) \right| \\
&\leq \sum_{i=1}^{n} \left| a_i \prod_{j=1}^{\eta} X_j^{e_j} \right| \leq \sqrt{n} \cdot \|f(x_1X_1,\ldots,x_\eta X_\eta)\| \\
&< M.
\end{aligned}$$

Since $f(\hat{x}_1, \ldots, \hat{x}_\eta) \equiv 0 \bmod M$, the result follows. $\square$

If the conditions in Howgrave-Graham's theorem are satisfied for each polynomial, we then have η polynomials that have $\hat{\mathbf{x}}$ as a root over the integers. Of course, the conditions in Howgrave-Graham's theorem are not necessary for $f(\hat{x}_1, \ldots, \hat{x}_\eta) = 0$ to hold over the integers. When each polynomial does have $\hat{\mathbf{x}}$ as a root over the integers we have a system of η equations in η unknowns that has at least one (integral) solution. If $\eta = 1$ we simply use standard root finding techniques to find $\hat{\mathbf{x}}$. If $\eta \geq 2$ however, we are not guaranteed to be able to solve the system of, presumably nonlinear, equations.

When the polynomials are algebraically independent, we can use resultant computations to construct a family of polynomials $g_{i,j}$ such that for each $i = 1, \ldots, \eta - 1$ and $j = 1, \ldots, i$ we have $g_{i,j} : g_{i,j}(x_1, \ldots, x_i)$ and $g_{i,j}(\hat{x}_1, \ldots, \hat{x}_i) = 0$. Starting with $g_{1,1}$ we can solve for $\hat{x}_1$ (which will be one of its integral roots) and back-substitute into one of the $g_{2,j}$ to solve for $\hat{x}_2$. We keep solving for roots of univariate polynomials and back-substituting until all of the desired roots are found.

When the polynomials are algebraically dependent, however, it is usually thought that this method cannot work. In general it doesn't work because the resultant of two algebraically dependent polynomials is always zero. In some special cases this algebraic dependence can be removed though. For example, suppose $g_1(x, y) = g(x, y) \cdot \hat{g}_1(x, y)$ and $g_2(x, y) = g(x, y) \cdot \hat{g}_2(x, y)$ where $\hat{g}_1$ and $\hat{g}_2$ are algebraically independent and $(\hat{x}, \hat{y})$ is common root we want to find. If it happens that $\hat{g}_1(\hat{x}, \hat{y}) = \hat{g}_2(\hat{x}, \hat{y}) = 0$ then we can simply use $\hat{g}_1$ and $\hat{g}_2$ instead of g_1 and g_2. And, the $\hat{g}_i$ are easily computed by $\hat{g}_i = g_i / \gcd(g_1, g_2)$. Unfortunately, if it happens that the common root is only a root of $g(x, y)$ then there is no known method of finding $\hat{x}$ and $\hat{y}$.

There is currently very little theory to predict which lattices will result in algebraically independent reduced basis vectors. For this reason, whenever $\eta > 1$, this method is only heuristic. Since we use multivariate polynomials ($\eta > 1$) in the attacks presented here, most of the results obtained are only heuristic. Because of this, we consider any attack using this method as successful if the lattice reduction yields η polynomials that each have $\hat{\mathbf{x}}$ as a root over the integers.

In [3], Blömer and May make the assumption that all the resultant computations for the multivariate polynomials constructed in their approaches yield non-zero polynomials. This is in fact not true. But, by removing the common factors of the polynomials before computing the resultants we have found that the resultant computations are non-zero. So, based on our experimental observations, we will use the following assumption throughout the rest of this work.

Assumption 1. *The resultant computations for the multivariate polynomials constructed in these approaches yield non-zero polynomials whenever these polynomials satisfy have* $\hat{\mathbf{x}}$ *as a root over the integers.*

It is interesting to note that there have been very few reported instances

(in cryptographic applications) of Coppersmith's method for modular multivariate polynomials resulting in algebraically dependent reduced basis vectors (see Blömer and May [2] for one such example). In light of the observations in this work, it might be the case that this lack of reported instances is simply due to a lack of experimental observations.

2 Most Significant Bits Known

In Section 4 of [3], Blömer and May present the first partial key attack on RSA with known most significant bits for public exponent $e > N^{1/2}$. Their main result is as follows.

Theorem 3 (Blömer-May [3]). *Under Assumption 1, for every $\epsilon > 0$ there exists an integer N_0 such that for every $N > N_0$ the following holds: Let (N, e) be an RSA public key, where $\alpha = \log_N(e)$ is in the range $[\frac{1}{2}, \frac{\sqrt{6}-1}{2}]$. Given an approximation $\tilde{d}$ of d with*

$$|d - \tilde{d}| \leq N^{\frac{1}{8}(5-2\alpha-\sqrt{36\alpha^2+12\alpha-15})-\epsilon}.$$

Then N can be factored in time polynomial in $\log N$.

As with most attacks on RSA using Coppersmith's method, the result is asymptotic in the size of the RSA modulus and the size of the lattice used in the attack. The attack results in a total break of RSA since the factorization of the modulus immediately yields the private key. The attack extends easily to multi-prime RSA. When there are more than two primes in the modulus the attack still results in a total break of RSA, however, the attack does not factor the modulus. Instead, the attack reveals the unknown portion of the private exponent. It also reveals Euler's totient function of the modulus which can be used to compute the private exponent or probabilistically factor the modulus (see [9]). An outline of the their attack (generalized for multi-prime RSA) is given below.

2.1 The Attack

Let's start with the public/private key equation $ed - k\phi(N) = 1$, where k is some positive integer. Let $\tilde{d}$ be our approximation of the private exponent satisfying $|d - \tilde{d}| \leq N^{\delta_0}$. With $\tilde{d}$ we compute an approximation of k as[1] $\tilde{k} = \frac{e\tilde{d}-1}{N}$. Writing $d = \tilde{d} + d_0$, $k = \tilde{k} + k_0$, and using $\phi(N) = N - \Lambda$, we rewrite the public/private key equation as

$$e(\tilde{d} + d_0) - (\tilde{k} + k_0)(N - \Lambda) = 1,$$

where d_0, k_0, and Λ are the only unknowns. Rearranging the terms, we obtain

$$ed_0 + (\tilde{k} + k_0)\Lambda + e\tilde{d} - 1 = (\tilde{k} + k_0)N.$$

[1] Blömer and May use $\tilde{k} = \frac{e\tilde{d}-1}{N-1}$ to approximate k.

This equation yields the trivariate polynomial

$$f_N(x, y, z) = ex + (\tilde{k} + y)z + e\tilde{d} - 1,$$

which contains the root $(x_0, y_0, z_0) = (d_0, k_0, \Lambda)$ modulo N. Since

$$|d_0| = |d - \tilde{d}| \leq N^{\delta_0},\ |k_0| = |k - \tilde{k}|, \text{ and } \Lambda \leq (2r-1)N^{1-1/r},$$

we can define bounds $X = N^{\delta_0}, Y$, and $Z = N^{\log_N(2r-1)+1-1/r}$ so that $|x_0| \leq X, |y_0| \leq Y$, and $|z_0| \leq Z$. The bound Y will be determined later. The polynomial $f_N(x, y, z)$ is then used to construct new polynomials that all have (x_0, y_0, z_0) as a root modulo N^m, for some positive integer m. We define the xz-shift and xy-shift polynomials of f_N: $g_{i,j,k}(x, y, z)$ and $h_{i,j,k}(x, y, z)$, respectively, as follows:

$$\begin{aligned} g_{i,j,k} &= x^{j-k} z^k N^i f_N^{m-1} && \text{for } i = 0, \ldots, m;\ j = 0, \ldots, i;\ k = 0, \ldots, j \\ h_{i,j,k} &= x^j y^k N^i f_N^{m-1} && \text{for } i = 0, \ldots, m;\ j = 0, \ldots, i;\ k = 1, \ldots, t \end{aligned}$$

where m and t are fixed parameters (to be determined). The coefficient vectors of the polynomials $g_{i,j,k}(xX, yY, zZ)$ and $h_{i,j,k}(xX, yY, zZ)$, which are linearly independent, are used to form a basis $B(m, t)$ for a lattice $L(m, t)$. The coefficient vector of each polynomial corresponds to a vector in $B(m, t)$. For given parameters m and t it is simple (if not tedious) to show that the lattice $L(m, t)$ has dimension

$$n = \dim(L) = (m+1)\,(m+2)\,(m+3+3\,t)\,/6,$$

and determinant (volume)

$$\det(L) = X^{C_X} Y^{C_Y} Z^{C_Z} N^{C_N},$$

where

$$\begin{aligned} C_X &= m\,(m+1)\,(m+2)\,(m+4\,t+3)\,/24, \\ C_Y &= (m+1)\,(m+2)\left(m^2 + 4\,tm + 3\,m + 6\,t^2 + 6\,t\right)/24, \\ C_Z &= m\,(m+1)\,(m+2)\,(m+2\,t+3)\,/24, \\ C_N &= m\,(m+1)\,(m+2)\,(3\,m+8\,t+9)\,/24. \end{aligned}$$

Each vector in the lattice $L(m, t)$ corresponds to the coefficient vector of some polynomial that has a root (x_0, y_0, z_0) modulo N^m. Using the LLL-lattice basis reduction algorithm we then find a reduced basis $(v_1', \ldots, v_n')$ for $L(m, t)$. From Theorem 1, we know that

$$\|v_1'\| \leq \|v_2'\| \leq \|v_3'\| \leq 2^{\frac{n+1}{4}} \det(L)^{\frac{1}{n-2}}.$$

To apply Howgrave-Graham's theorem, these first three vectors in the reduced basis must satisfy $\|v_i'\| < \frac{N^m}{\sqrt{n}}$ for $i = 1, 2, 3$. This condition is guaranteed if

$$2^{\frac{n+1}{4}} \det(L)^{\frac{1}{n-2}} < \frac{N^m}{\sqrt{n}}.$$

Thus, a sufficient condition is

$$\det(L) < \frac{N^{m(n-2)}}{2^{\frac{(n+1)(n-2)}{4}} n^{\frac{n-2}{2}}}. \tag{4}$$

If (4) is satisfied, then the three polynomials whose coefficient vectors are v_1', v_2', and v_3' each have (x_0, y_0, z_0) as a root over the integers. We then use resultant computations to remove variables from the polynomials until we have one univariate polynomial in x. One of the integer roots of this polynomial will be d_0, which then yields the entire private exponent $d = \tilde{d} + d_0$.

Thus, we have an algorithm that takes (N, e), $\tilde{d}$, X, Y, Z, m, and t as input and outputs (N, d) if inequality (4) is satisfied. Of course, since the bounds in Theorem 1 are not very tight the attack may still be successful even if (4) is not satisfied. Indeed, as long as the three polynomials whose coefficient vectors are v_1', v_2', and v_3' satisfy the Howgrave-Graham condition the attack will work.

2.2 Multi-prime RSA

When extending the attack to multi-prime RSA, we obtain the following result.

Theorem 4. *Under Assumption 1, for every $\epsilon > 0$ and every integer $r \geq 2$ there exists an integer N_0 such that for every $N > N_0$ the following holds: Let (N, e) be an r-prime RSA public key, where $\alpha = \log_N(e)$ is in the range*

$$\frac{1}{r} < \alpha \leq \frac{4 - 3\,r + \sqrt{9\,r^2 - 12\,r + 12}}{2\,r},$$

and $\tilde{d} = N^{\tilde{\delta}}$ be a known approximation of the private exponent d with $|d - \tilde{d}| \leq N^{\delta_0}$, such that

$$\delta_0 \leq \frac{5 - \alpha\,r - \sqrt{3\,(\alpha\,r - 1)\,(3\,\alpha\,r + 8\,r + -11)}}{4\,r} - \epsilon,$$

and

$$\delta_0 \leq \tilde{\delta} - \frac{1}{r}.$$

Then the private key (N, d) can be fully recovered in time polynomial in $\log N$.

For the first few values of r, plots showing the fraction of MSBs required for all valid α values are shown in Figure 1. The area above each curve, which we will call the *sufficient region*, represents the region where the attack is guaranteed to work. That is, the conditions in Howgrave-Graham's Theorem are satisfied for each (α, δ_0) pair that lies in the sufficient region (for asymptotically large modulus and lattice dimension). Notice that the sufficient region decreases with each additional prime in the modulus.

Proof (Theorem 4). Using the attack described in Section 2.1, we begin by computing a bound for Y. For r-prime RSA, using $\tilde{k} = \frac{e\tilde{d}-1}{N}$ to approximate k, we

Partial Key Exposure Attack with known Most Significant Bits

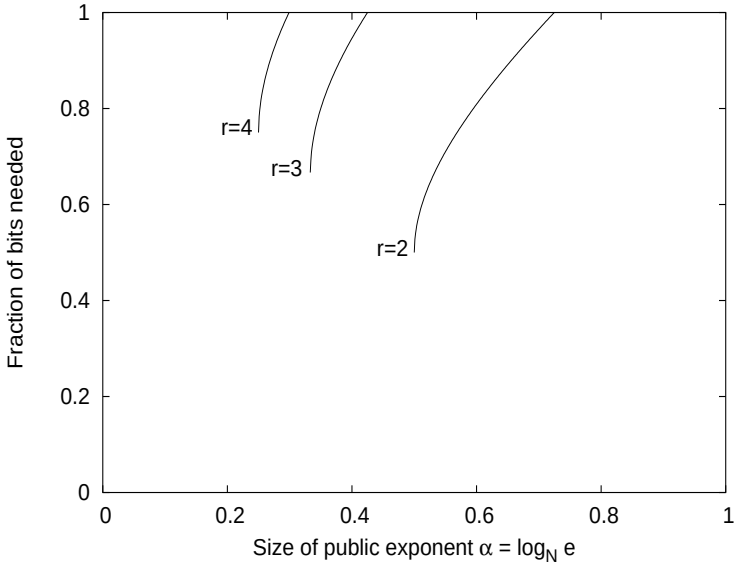


FIGURE 1: Lower bounds of the fraction of MSBs required for the attack for large modulus.

have that

$$\begin{aligned}
|k-\tilde{k}| &= \left|\frac{ed-1}{\phi(N)} - \frac{e\tilde{d}-1}{N}\right| = \left|\frac{(ed-1)N-(e\tilde{d}-1)\phi(N)}{\phi(N)N}\right| \\
&= \left|\frac{(ed-1)N-(e\tilde{d}-1)(N-\Lambda)}{\phi(N)N}\right| = \left|\frac{e(d-\tilde{d})}{\phi(N)}\right| + \left|\frac{(e\tilde{d}-1)\Lambda}{\phi(N)N}\right| \\
&\leq \frac{e}{\phi(N)}\left|(d-\tilde{d})\right| + \frac{e}{\phi(N)}\frac{\tilde{d}\Lambda}{N} = \frac{e}{\phi(N)}\left(\left|(d-\tilde{d})\right| + \frac{\tilde{d}\Lambda}{N}\right) \\
&\leq \frac{e}{\phi(N)}\left(N^{\delta_0} + (2r-1)\tilde{d}N^{-1/r}\right). \qquad (5)
\end{aligned}$$

Since $\delta_0 \leq \tilde{\delta} - \frac{1}{r}$, inequality (5) becomes

$$|k-\tilde{k}| < \frac{e}{\phi(N)} 2r\tilde{d}N^{-1/r} = N^{\alpha-(1-\lambda)+\log_N(2r)+\tilde{\delta}-\frac{1}{r}}. \qquad (6)$$

Thus, for this attack we have the following bounds:

$$|d_0| \leq N^{\delta_0}, \quad |k_0| \leq 2rN^{\alpha-(1-\lambda)+\tilde{\delta}-\frac{1}{r}}, \quad |\Lambda| \leq (2r-1)N^{1-\frac{1}{r}}. \qquad (7)$$

For large N, all $\log_N(\cdot)$ terms and λ are negligible in the exponents and can be ignored. Also, since $\tilde{\delta} < 1$ (i.e., $\tilde{d} < N$) we can define

$$X = N^{\delta_0}, \quad Y = N^{\alpha-\frac{1}{r}}, \quad Z = N^{1-\frac{1}{r}},$$

so that $|d_0| \leq X$, $|k_0| \leq Y$, and $|\Lambda| \leq Z$. Following Blömer and May, we introduce the parameter τ by letting $t = \tau\, m$ and rewrite everything in terms of m:

$$\begin{aligned} m(n-2) &= m^4(12\tau+4)(1+o(1))/24, \\ C_X &= m^4(4\tau+1)(1+o(1))/24, \\ C_Y &= m^4(6\tau^2+4\tau+1)(1+o(1))/24, \\ C_Z &= m^4(4\tau+2)(1+o(1))/24, \\ C_N &= m^4(8\tau+3)(1+o(1))/24. \end{aligned}$$

The determinant of the lattice becomes

$$\det(L) = \left(X^{4\tau+1}Y^{6\tau^2+4\tau+1}Z^{4\tau+2}N^{8\tau+3}\right)^{m^4(1+0(1))/24}.$$

Using the bounds $X = N^{\delta_0}, Y = N^{\alpha-1/r}$, and $Z = N^{1-1/r}$ we then have

$$\det(L) = N^{\frac{1}{24}m^4\left(6(\alpha-\frac{1}{r})\tau^2+4(\alpha+\delta_0+3-\frac{2}{r})\tau+\alpha+\delta_0+5-\frac{3}{r}\right)(1+o(1))}.$$

For large modulus and lattice size ($N, m \to \infty$) we can neglect all low order terms of m and terms that do not depend on N explicitly. The condition to apply Howgrave-Graham's theorem, inequality (4), then becomes

$$6\left(\alpha-\frac{1}{r}\right)\tau^2 + 4\left(\alpha+\delta_0-\frac{2}{r}\right)\tau + \left(\alpha+\delta_0+1-\frac{3}{r}\right) < 0. \tag{8}$$

When $\alpha - \frac{1}{r} > 0$, the left hand side of (8) is minimized when

$$\tau = -\frac{\alpha+\delta_0-\frac{2}{r}}{3(\alpha-\frac{1}{r})}.$$

Upon substituting this value for τ into (8), and solving for δ_0, we obtain

$$\delta_0 < \frac{5-\alpha\,r-\sqrt{3\,(\alpha\,r-1)\,(3\,\alpha\,r+8\,r+-11)}}{4\,r}.$$

Finally, setting $\delta_0 = 0$ in (9) and solving for α yields

$$\alpha \leq \frac{4-3\,r+\sqrt{9\,r^2-12\,r+12}}{2\,r},$$

which concludes the proof. □

For the first few r values, Table 2 shows the upper bound on δ_0 so that the conditions in Howgrave-Graham's Theorem are satisfied for its corresponding range of public exponents. Letting $r = 2$ gives the same results that Blömer and May report for RSA.

In extending the attack to multi-prime RSA we have added the additional condition $\delta_0 \leq \tilde{\delta} - \frac{1}{r}$. Blömer and May observe that if $\delta_0 > \tilde{\delta} - \frac{1}{2}$ in RSA then N can be factored. Their result extended to the general multi-prime case is summarized in the following.

r	$\alpha = \log_N(e)$	δ_0^{max}
2	$\left[\frac{1}{2}, \frac{\sqrt{6}-1}{2}\right]$	$\frac{1}{8}(5 - 2\,\alpha - \sqrt{36\,\alpha^2 + 12\,\alpha - 15})$
3	$\left[\frac{1}{3}, \frac{\sqrt{57}-5}{6}\right]$	$\frac{1}{12}(5 - 3\,\alpha - \sqrt{81\,\alpha^2 + 90\,\alpha - 39}))$
4	$\left[\frac{1}{4}, \frac{3\sqrt{3}-4}{4}\right]$	$\frac{1}{16}(5 - 4\,\alpha - \sqrt{144\,\alpha^2 + 216\,\alpha - 63}))$

TABLE 2: For each r value and public exponent in the given range, the last column gives the upper bound on δ_0 so that conditions in Howgrave-Graham's Theorem are satisfied.

Theorem 5. *For every integer $r \geq 2$ the following holds: Let (N, e) be an r-prime RSA public key, where $\alpha = \log_N(e)$, and let $\tilde{d} = N^{\tilde{\delta}}$ be a known approximation of the private exponent d such that $|d - \tilde{d}| = N^{\delta_0}$. If the inequalities*

$$\delta_0 > \tilde{\delta} - \frac{1}{r}, \quad \alpha + \delta_0 < 1 - \log_N(2) - \lambda, \quad \textit{and} \quad \alpha > 1 - \frac{1}{r} + \log_N(2r-1), \tag{9}$$

are all satisfied then the private key (N, d) can be fully recovered in time polynomial in $\log N$.

Proof (Theorem 5). Since $\delta_0 > \tilde{\delta} - \frac{1}{r}$ and $\alpha + \delta_0 < 1 - \log_N(2) - \lambda$ we completely know k since $|k - \tilde{k}| \leq N^{\alpha - 1 + \lambda + \log_N(2) + \delta_0} < 1$. Computing $k^{-1} \bmod e$ allows us to compute $\Lambda = N - k^{-1} \bmod e$. Since $\alpha > 1 - \frac{1}{r} + \log_N(2r-1)$ we have that $e > \Lambda$ and so we have computed Λ over the integers. The result follows. □

In practise, however, this theorem is of very little use except when $r = 2$. In general, when computing the public/private exponents either $e \approx N$, $d \approx N$, or both. Under the assumption that at least one of these exponents is of the order of N we see that this attack can only work under very special circumstances for $r > 2$. To see this, first notice that the three conditions in the theorem imply that

$$1 + \tilde{\delta} - 2/r + \log_N(2r-1) < \alpha + \delta_0 < 1 - \log_N(2) - \lambda,$$

which in turn implies that $\tilde{\delta} < \frac{2}{r}$. Since $\tilde{\delta} \approx \delta$, we must have $\delta \lessapprox \frac{2}{r}$, so if $r > 2$ then $d \not\approx N$. Assuming then that $e \approx N$, the first two conditions of (9) imply that $\tilde{\delta} \approx \frac{1}{r}$. Again, since $\tilde{\delta} \approx \delta$, the attack will only be successful when $d \approx N^{1/r}$. So, for $r > 2$, the attack only works for a very narrow range of private exponents.

2.3 Experimental Results

The results of Section 2.2 are asymptotic in the size of the modulus and the size of the lattice used. To illustrate the practical effectiveness of the attack we carried some experiments to approximate a lower bound on the number of MSBs

needed to mount the attack for various lattice dimensions. The method used to approximate these bounds is as follows. For each value of r, modulus size and public exponent size (α), a new random modulus and valid public exponent ($e \approx N^{\alpha}$, $\gcd(e, \phi(N)) = 1$) were computed. We then carried out a binary search on values of δ_0 that resulted in a successful attack. The search was terminated when the difference between δ_0 for a successful attack and an unsuccessful attack was less than some given tolerance (we used 0.0025 for all our experiments). The criterion of a successful attack changed over the course of the experiments. At the beginning, an attack was deemed successful only if we recovered d_0 (and hence d) by finding all the integer roots of a univariate polynomial obtained from the resultant computations on the three smallest polynomials found from the lattice basis reduction. As the lattice dimensions and modulus sizes were increased, we found that the time to perform the resultant computations were becoming prohibitive for our purposes, since the attack is repeated many times for each public exponent. To reduce the total time for each attack, we changed the criterion so that an attack is successful if from the lattice basis reduction we could construct three algebraically independent polynomials that all have $(x, y, z) = (d_0, k_0, \Lambda)$ as a root over the integers. The lattice reductions were performed using Shoup's NTL [15] while all other computations (polynomial manipulation, resultants, and integer root solving) were done with Maple9 [13].

Figure 2 shows the results for RSA with a 1024-bit modulus. As can been

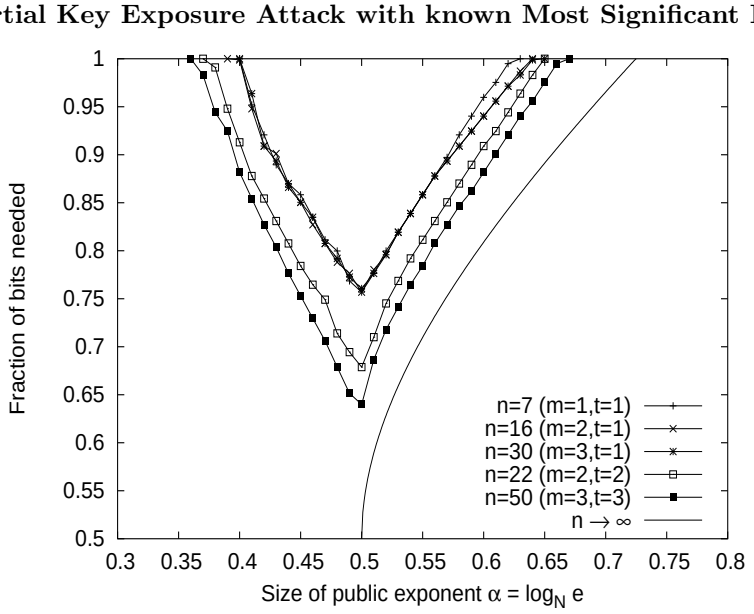


FIGURE 2: Experimental lower bounds of the fraction of MSBs required to attack RSA with a 1024-bit modulus.

seen, even for small lattice dimensions ($n \leq 50$) the attack is quite successful.

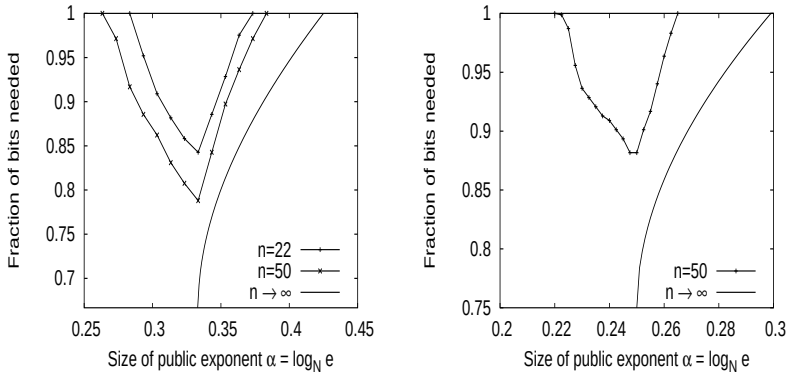
Another observation, is that that attack also works for public exponent $e < N^{1/2}$. In general, we find that for r-prime RSA, the attacks will work for public exponents $e < N^{1/r}$. While we can explain why the attack should work for $\alpha < 1/r$, we cannot explain the behaviour of δ_0 with α. Briefly, when $\alpha < 1/r$ we have the bound $Y = 2r$ (recall that we used the bound $Y = 2rN^{\alpha-1/r}$ in the attack). Now consider inequality (5) once more:

$$|k - \tilde{k}| \leq \frac{e}{\phi(N)} \left(N^{\delta_0} + (2r-1)\tilde{d}N^{-1/r} \right).$$

When $\alpha < 1/2$ and $\alpha + \delta_0 < 1 - \lambda$ we have $\frac{N^{\alpha+\delta_0}}{\phi(N)} \leq 1$ and $\frac{e\tilde{d}N^{-1/2}}{\phi(N)} \leq 1$ so that $|k - \tilde{k}| \leq 2r$. Thus, $Y = 2r$ is a valid bound and the attack should still work (provided that the lattice basis reduction yields three algebraically independent polynomials that have $(x, y, z) = (d_0, k_0, \Lambda)$ as root over the integers).

Results for $r = 3$ with a 2048-bit modulus and $r = 4$ with a 4096-bit modulus are shown in Figure 3. The data shows similar trends to RSA with a 1024-

Partial Key Exposure Attack with known Most Significant Bits



(a) 2048-bit Modulus, $r = 3$ (b) 4096-bit Modulus, $r = 4$

FIGURE 3: Experimental lower bounds of the fraction of MSBs required to attack multi-prime RSA. (a) 3-prime RSA with 2048-bit modulus. (b) 4-prime RSA with 4096-bit modulus.

bit modulus. It is interesting to note, however, that with larger values of r larger lattices were needed for a successful attack. For $r = 3$, lattices with $(m, t) \in \{(1, 1), (2, 1), (3, 1)\}$ were completely unsuccessful as were all lattices with $m + t \leq 4$ for $r = 4$.

The data also shows that the experimental bounds for the fraction of MSBs needed changes only slightly with the modulus sizes used. The attack seems to become slightly stronger with increasing modulus size but this increase is not significant. Table 3 shows some typical results. Since the modulus sizes that we consider do not vary greatly, this is not unexpected. In general, the data shown in Figures 2 and 3 are representative of all the experiments carried out.

$\log_2 N$	1024	2048	4096	8192	
$r = 2$	0.694	0.694	0.691	0.671	$m = t = 2$, $\alpha = 1/2$
$r = 3$	0.792	0.788	0.784	-	$m = t = 3$, $\alpha = 1/3$

TABLE 3: Approximate lower bound of fraction of MSBs needed for the attack with respect to different modulus sizes.

2.4 Algebraic Dependence

Coppersmith's method for finding small roots of multivariate polynomials over the integers is a heuristic. This is because at present one cannot predict when the polynomials obtained from the LLL algorithm will be algebraically independent or not and because we have no current method of solving a system of nonlinear polynomials that are algebraically dependent. In most cryptographic applications however, there are very few reported instances of the method yielding algebraically dependent polynomials. In our experiments implementing Blömer and May's partial key exposure attack (on RSA and multi-prime RSA) we have found many instances when the three polynomials obtained from the LLL algorithm are indeed algebraically dependent, but can still be used to find d_0. In these cases, simply dividing each polynomial by the greatest common divisor of the three polynomials resulted in three algebraically independent polynomials that still had $(x, y, z) = (d_0, k_0, \Lambda)$ as a root over the integers.

2.5 Non-Asymptotic Bounds

It is well known that the size of the vectors obtained from the LLL algorithm can be much smaller than what the current theory predicts. To illustrate this, we compare the experimental lower bounds obtained in Section2.3 with what the theory tells us for some particular lattice parameters. The theory gives us the following sufficient condition for the attack to work:

$$\det(L) < 2^{-\frac{(n+1)(n-2)}{4}} n^{-\frac{n-2}{2}} N^{m(n-2)}.$$

In the asymptotic case, the the term $2^{-\frac{(n-1)(n-2)}{4}} n^{-\frac{n-2}{2}}$ is ignored, as it does not explicitly depend on N and truly is insignificant as $N \to \infty$ for any fixed n. However, for a 1024-bit modulus, mounting the attack with a lattice of dimension $n = 50$ (using $m = t = 3$), we see that

$$2^{-\frac{(n+1)(n-2)}{4}} n^{-\frac{n-2}{2}} = N^{-\frac{(n+1)(n-2)}{4}\log_N(2) - \frac{n-2}{2}\log_N(n)} \approx N^{-0.73},$$

which is quite a large contribution. If we do not neglect any terms and use specific lattice parameters, what we find is that the theoretical sufficient condition on δ_0 is not very indicative of the attacks actual strength. For example, when the lattice parameters satisfy $m + t \leq 4$, the theoretical sufficient condition is that $\delta_0 \leq 0$. Thus, in order to obtain all of d the attacked must have already had all of d. This holds for all values of r and N considered. When $m + t > 4$,

the theory does give some non-zero bounds for δ_0. Figure 4 shows the bounds on the fraction of MSBs for RSA with a 1024-bit modulus using lattice parameters $m = t = 3$. As can be seen, the actual attack is much stronger than

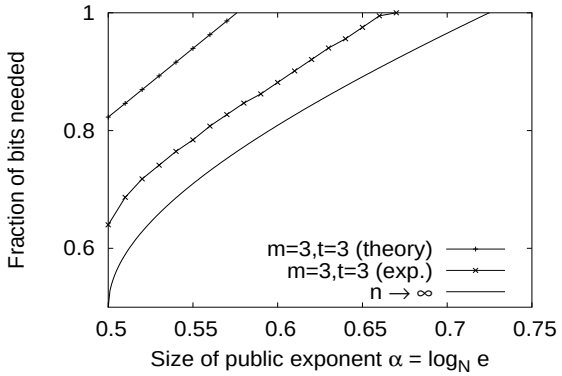


FIGURE 4: Lower bounds for MSBs. Comparison of theoretical and experimental results for RSA with 1024-bit modulus using lattice parameters $m = t = 3$. The asymptotic theoretical sufficient condition is also shown.

what the theoretical sufficient conditions indicate. The experimental evidence seems to suggest that the asymptotic bounds are actually a good reflection of the strength of the attack.

3 Least Significant Bits Known I

Blömer and May present two partial key attacks with known least significant bits. The first attack (Section 5 in [3]) is a provable method for most public exponents $e < N^{1/2}$. The main result of their attack is as follows.

Theorem 6 (Blömer and May [3]). *Let N be an RSA-modulus and let $0 < \alpha, \epsilon < \frac{1}{2}$. For all but a $\mathcal{O}(\frac{1}{N^\epsilon})$-fraction of the public exponents e in the interval $[3, N^\alpha]$ the following holds: Let d be the private exponent. Given d_0 and M satisfying $d = d_0 \bmod M$ and*

$$N^{\alpha+\frac{1}{2}+\epsilon} \leq M \leq 2\, N^{\alpha+\frac{1}{2}+\epsilon},$$

the factorization of N can be found in polynomial time.

The attack is successful for all but $\mathcal{O}(N^{\alpha-\epsilon})$ public exponents in the range $[3, N^\alpha]$. Of course, this is only an upper bound on the number of public exponents that may thwart the attack; it does not indicate the actual number of public exponents that do so. When $\epsilon \geq \alpha$ this upper bound shows that the attack is almost always successful (no matter the public exponent used). If $\epsilon < \alpha$, however, the bound may be a large fraction of the total possible public

exponents. For convenience, we will call these public exponents for which the attack is not successful *bad public exponents*.

3.1 Multi-prime RSA

In the multi-prime RSA setting, we find that the attack is guaranteed to work for all but $\mathcal{O}(N^{1+\alpha-\frac{2}{r}-\epsilon})$ of the public exponents in the range $[3, N^\alpha]$. Simply extending the attack on RSA to multi-prime RSA we obtain the following result.

Theorem 7. *Let N be an r-prime RSA-modulus and let $0 < \alpha, \epsilon < 1 - \frac{1}{r}$ such that $\alpha + \epsilon + \frac{1}{r} < 1$. For all but a $\mathcal{O}(N^{1-2/r-\epsilon})$-fraction of the public exponents e in the interval $[3, N^\alpha]$ the following holds: Let d be the private exponent. Given d_0 and M satisfying $d = d_0 \bmod M$ and*

$$N^{\alpha+\frac{1}{r}+\epsilon} \leq M \leq 2\, N^{\alpha+\frac{1}{r}+\epsilon},$$

the private exponent can be recovered in polynomial time.

As stated, the attack can be mounted against multi-prime RSA with public exponent $e < N^{1-\frac{1}{r}}$. If the attack is successful for most public exponents in this range it would be the first attack that becomes stronger as r increases[2]. This is not the case though. For the attack to be useful, the bound on the number of bad public exponents must be small. To ensure this, we force $\epsilon > 1 - \frac{2}{r}$, so that the number of bad exponents is $\mathcal{O}(1)$. Since $\alpha + \epsilon + \frac{1}{r} < 1$, this implies that $\alpha < \frac{1}{r}$. So, while the attack theoretically works for larger public exponent ranges as r increases, the actual useful range decreases. Before proving this theorem, we state a corollary which reflects the practical nature of the theorem.

Corollary 1. *Let N be an r-prime RSA-modulus and let α, ϵ satisfy $0 < \alpha < \frac{1}{r}$, $1 - \frac{2}{r} < \epsilon < 1 - \frac{1}{r}$, and $\alpha + \epsilon + \frac{1}{r} < 1$. For all but a $\mathcal{O}(1)$-fraction of the public exponents e in the interval $[3, N^\alpha]$ the following holds: Let d be the private exponent. Given d_0 and M satisfying $d = d_0 \bmod M$ and*

$$N^{1+\alpha-\frac{1}{r}} \leq N^{\alpha+\frac{1}{r}+\epsilon} \leq M \leq 2\, N^{\alpha+\frac{1}{r}+\epsilon},$$

the private exponent can be recovered in polynomial time.

Figure 5 shows the lower bounds on the fraction of LSBs needed for the first few values of r to guarantee success of this attack (using the criteria of the corollary). With each additional prime in the modulus, the sufficient region decreases. This trend continues for larger values of r.

We now give a proof of the theorem (the corollary follows directly from the theorem). This proof follows Blömer and May's proof for RSA closely.

Proof (Theorem 7). Again, we begin with the public/private key equation $ed - k\phi(N) = 1$, where k is some positive integer. Writing $d = d_1 M + d_0$ and $\phi(N) = N - \Lambda$ we have

$$ed_1 M + k\Lambda - 1 + ed_0 = kN,$$

[2]With respect to the range of public exponent that the attack works for.

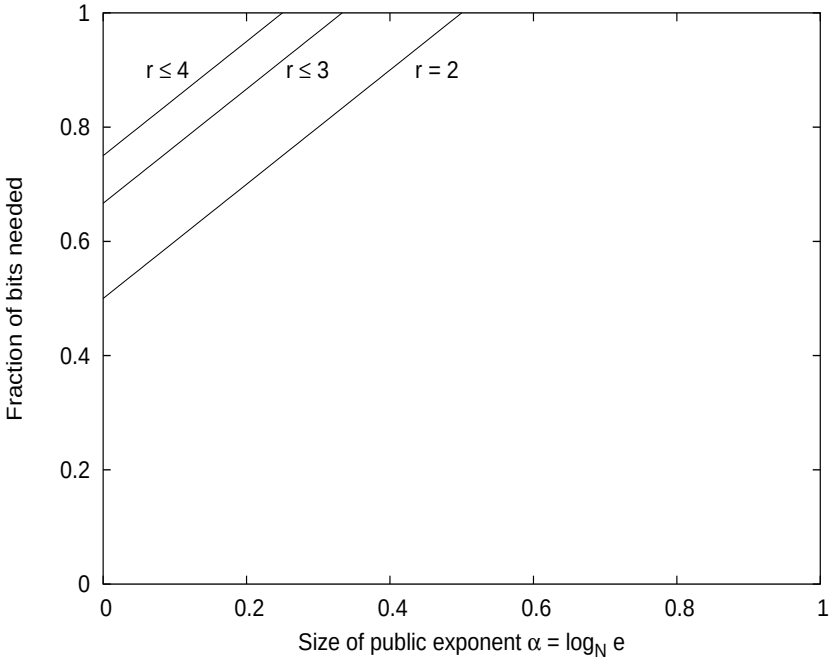


FIGURE 5: Lower bounds for the fraction of least significant bits needed for the attack.

where d_1, k, and Λ are the only unknowns. This equation yields the bivariate polynomial

$$f_N(x, y) = eMx + y + ed_0,$$

which contains the root $(x_0, y_0) = (d_1, k\Lambda - 1)$ modulo N. It is also important to notice that $f_N(x_0, y_0) = kN$. Now, $d = d_1M + d_0 < N$ so we can bound d_1 above by $\frac{N}{M} \leq N^{1-\alpha-1/r-\epsilon}$. Also, since $k < e$, we can bound $k\Lambda - 1$ above by $(2r-1)N^{\alpha+1-1/r}$. Thus, defining $X = N^{1-\alpha-1/r-\epsilon}$ and $Y = (2r-1)N^{\alpha+1-1/r}$ we have $x_0 \leq X$ and $y_0 \leq Y$.

With the introduction of the auxiliary polynomials N and Nx, we then consider the lattice spanned by the coefficient vectors of N, NxX, and $f_N(xX, yY)$. That is, we consider the lattice spanned by

$$B = \begin{bmatrix} N & & \\ & NX & \\ ed_0 & eMX & Y \end{bmatrix}.$$

Notice that each vector in the lattice spanned by B corresponds to a polynomial of the form

$$f = a_0N + a_1Nx + a_2f_N(x, y),$$

and that each of these polynomials has the root (x_0, y_0) modulo N. Further, Howgrave-Graham's theorem tells us that each such polynomial that has norm smaller than $N/\sqrt{3}$ has the root (x_0, y_0) over the integers.

So, if we can find two vectors in the lattice, $(a_0, a_1, a_2)B$ and $(b_0, b_1, b_2)B$ say, that are linearly independent and have norm smaller than $\frac{N}{\sqrt{3}}$ then we can apply Howgrave-Graham's theorem to obtain the following equations:

$$\begin{aligned} a_0\ N + a_1\ Nx_0 + a_2\ f_N(x_0, y_0) &= 0 \\ b_0\ N + b_1\ Nx_0 + b_2\ f_N(x_0, y_0) &= 0. \end{aligned}$$

Since $f_N(x_0, y_0) = kN$, we then have the following system of equations

$$\begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix} \begin{pmatrix} x_0 \\ k \end{pmatrix} = - \begin{pmatrix} a_0 \\ b_0 \end{pmatrix},$$

which we can solve for x_0 and k since (a_1, a_2) and (b_1, b_2) are linearly independent. That (a_1, a_2) and (b_1, b_2) are linearly independent follows from (a_0, a_1, a_2) and (b_0, b_1, b_2) being linearly independent. Since $x_0 = d_1$, we can reconstruct $d = d_1 M + d_0$ to obtain the entire private key.

All that remains is to find two linearly independent vectors with norm less than $\frac{N}{\sqrt{3}}$. Since the lattice dimension is 3, two shortest linearly independent vectors in the lattice can be found using an algorithm of Blömer [1]. The rest of the proof shows that for all choices of public exponent $e \in [3, N^\alpha]$, except at most $\mathcal{O}(N^{1-2/r-\epsilon})$, the two shortest vectors have norm smaller than $\frac{N}{\sqrt{3}}$.

Following Blömer and May, we move to a lattice theory framework. Let L denote the lattice spanned by B and λ_i be the i^{th} successive minima of L. We are interested in finding a bound on the number of public exponents in $[3, n^\alpha]$ such that the second minima λ_2 of L is strictly less than $\frac{N}{\sqrt{3}}$. These are the bad public exponents. Since $\dim(L) = 3$, Minkowski's second theorem tells us that

$$\lambda_1 \lambda_2 \lambda_3 \leq 2 \det(L).$$

For each public exponent, e, if $\lambda_1 > 6XY$ then the second minima satisfies $\lambda_2^2 \leq \lambda_2 \lambda_3 \leq \frac{2 \det(L)}{\lambda_1} \leq \frac{2N^2 XY}{6XY}$, since $\det(L) = N^2 XY$. Thus, $\lambda_2 < \frac{N}{\sqrt{3}}$. So, if any public exponent e is a bad exponent, it must be the case that $\lambda_1 \leq 6XY$. The remainder of this proof is now dedicated to bounding the number of public exponents that have $\lambda_1 \leq 6XY$.

To this end, let's assume that $\lambda_1 \leq 6XY$. Thus, there exists $c_0, c_1, c_2 \in \mathbb{Z}$ such that $\|(c_0, c_1, c_2)B\| \leq 6XY$. That is,

$$\|(c_0 N + c_2 e d_0), (c_1 NX + c_2 eMX), (c_2 Y)\| \leq 6XY.$$

This implies that

(i) $|c_2| \leq 6X$, and

(ii) $\left| \frac{c_1}{|c_2|} + \frac{c_2}{|c_2|} \frac{eM}{N} \right| \leq \frac{6Y}{|c_2| N}$.

Since $\frac{eM}{N}$ is positive we know that one of c_1 and c_2 is positive and one is negative. Further, since $\|(c_0, c_1, c_2)B\| = \|(-c_0, -c_1, -c_2)B\|$ we can, without loss of generality, assume that c_2 is positive. As a result, we can rewrite (ii) as $\left|\frac{c_1}{c_2} + \frac{eM}{N}\right| \leq \frac{6Y}{c_2 N}$. Using $XY = (2r-1)N^{2-\frac{2}{r}-\epsilon}$, condition (ii) then implies

$$\left|\frac{c_1}{c_2} + \frac{eM}{N}\right| \leq \frac{6(2r-1)}{c_2 X} N^{1-\frac{2}{r}-\epsilon}. \tag{10}$$

Now we find the maximum number of public exponents in the range $[3, N^\alpha]$ that can satisfy (10) for some (c_1, c_2). Blömer and May make the following observations (which we have slightly modified for multi-prime RSA):

- The difference between any two numbers of the form $\frac{eM}{N}$ (for different e values) is at least $\frac{M}{N} \geq N^{\alpha+1/r+\epsilon-1}$.
- If (10) is satisfies for some ratio $\frac{c_1}{c_2}$ and some e then $\frac{eM}{N}$ must satisfy

$$\frac{c_1}{c_2} - \frac{6(2r-2)}{c_2 X} N^{1-\frac{2}{r}-\epsilon} \leq \frac{eM}{N} \leq \frac{c_1}{c_2} + \frac{6(2r-2)}{c_2 X} N^{1-\frac{2}{r}-\epsilon}.$$

- The previous two observations imply that for a fixed ratio $\frac{c_1}{c_2}$ there are at most $\frac{12(2r-1)}{c_2 X} N^{2-\frac{3}{r}-\alpha-2\epsilon}$ public keys e such that (10) is satisfied.
- Consider a fixed (but arbitrary) c_2. Since $e \leq N^\alpha$ and $M \leq 2N^{\alpha+1/r+\epsilon}$ we have that $\frac{eM}{N} \leq 2N^{2\alpha+1/r+\epsilon}$. For some c_1 and public exponent e, inequality (10) can only be satisfied if $c_1 \in [-2N^{2\alpha+\frac{1}{r}-1+\epsilon} c_2, -1]$.
- The previous two observations imply that for a fixed c_2 the number of public exponents satisfying (10) is bound above by $\frac{24(2r-1)}{X} N^{1-\frac{2}{r}+\alpha-\epsilon}$.
- Since $c_2 \leq 6X$, the last observation implies that the number of public exponents for which (10) is satisfied for some ratio $\frac{c_1}{c_2}$ is bound above by $144(2r-1)\, N^{1+\alpha-\frac{2}{r}-\epsilon}$.

So, for fixed r, the number of bad public exponents in $[e, N^\alpha]$ is $\mathcal{O}(N^{1+\alpha-2/r-\epsilon})$, which concludes the proof. □

While Boneh, Durfee, and Frankel [4] had already discovered a polynomial-time partial key exposure attack against RSA with known least significant bits for public exponent polynomial in $\log_2 N$ (i.e., very small public exponents), this is the first known attack for public exponents as large as $N^{1/2}$. Also, since Boneh, Durfee, and Frankel's attack cannot be extended to multi-prime RSA, as demonstrated by Hinek, Low, and Teske [9], this is the first known such attack for multi-prime RSA. Perhaps even more important though, since a stronger (but heuristic) attack follows in the next section, is that this attack introduces a new method to solve modular multivariate polynomial equations of a special form.

4 Least Significant Bits Known II

The second partial key attack with known least significant bits in [3] (Section 6) uses Coppersmith's method with bivariate polynomials and so is only a heuristic. This attack is mountable for public exponents $e \leq N^{7/8}$. It is also the first known attack that works for public exponents $e > N^{1/2}$. Their main result is the following theorem.

Theorem 8 (Blömer-May [3]). *Under Assumption 1, for every $\epsilon > 0$ there exists N_0 such that for every $N \geq N_0$ the following holds: Let (N, e) be an RSA public key with $\alpha = \log_N(e) \leq \frac{7}{8}$. Let d be the private exponent. Given d_0 and M satisfying $d = d_0 \bmod M$ and*

$$M \geq N^{\frac{1}{6}+\frac{1}{3}\sqrt{1+6\ \alpha}+\epsilon},$$

the modulus N can be factored in polynomial time.

While this attack does require a larger fraction of the LSBs of the private exponent, as compared to Boneh, Durfee, and Frankel's [4], it works for a much larger range of public exponents. An outline of Blömer and May's attack (generalized for multi-prime RSA) is given below.

4.1 The Attack

Once again, we start with the public/private key equation $ed - k\phi(N) = 1$, where k is some positive integer. Writing $d = d_1 M + d_0$ and $\phi(N) = N - \Lambda$ we obtain

$$k(N - \Lambda) - ed_0 + 1 = eMd_1,$$

where k and Λ are the only unknowns on the left hand side. This leads to the bivariate polynomial

$$f_{eM}(y, z) = y(N - z) - ed_0 + 1,$$

which contains the root $(y_0, z_0) = (k, \Lambda)$ modulo eM. Since

$$k < e = N^{\alpha} \text{ and } \Lambda \leq (2r - 1)N^{1-1/r},$$

we can define the bounds $Y = N^{\alpha}$ and $Z = N^{1-1/r+\log_N(2r-1)}$ so that $|y_0| \leq Y$ and $|z_0| \leq Z$. The polynomial $f_{eM}(y, z)$ is then used to construct new polynomials that all have (y_0, z_0) as a root modulo $(eM)^m$, for some positive integer m. We define the y-shift and z-shift polynomials of f_N: $g_{i,j}(y, z)$ and $h_{i,j}(y, z)$, respectively, as follows:

$$\begin{aligned} g_{i,j} &= y^j (eM)^i f_{eM}^{m-1} \quad \text{for } i = 0, \ldots, m;\ j = 0, \ldots, i \\ h_{i,j} &= z^j (eM)^i f_{eM}^{m-1} \quad \text{for } i = 0, \ldots, m;\ j = 1, \ldots, t. \end{aligned}$$

where m and t are fixed parameters (to be determined). The coefficient vectors of the polynomials $g_{i,j}(yY, zZ)$ and $h_{i,j}(yY, zZ)$, which are linearly independent,

are used to form a basis $B(m,t)$ for a lattice $L(m,t)$. The coefficient vector of each polynomial corresponds to a vector in $B(m,t)$. For given parameters m and t, it is simple (if not tedious) to show that the lattice $L(m,t)$ has dimension

$$n = \det(L) = (m+1)\,(m+2\,t+2)\,/2,$$

and determinant (volume)

$$\det(L) = Y^{C_Y} Z^{C_Z} (eM)^{C_{eM}},$$

where

$$\begin{aligned} C_Y &= m\,(m+1)\,(2\,m+3\,t+4)\,/6, \\ C_Z &= (m+1)\left(m^2+2\,m+3\,tm+3\,t^2+3\,t\right)/6, \\ C_{eM} &= m\,(m+1)\,(2\,m+3\,t+4)\,/6. \end{aligned}$$

Each vector in the lattice $L(m,t)$ corresponds to the coefficient vector of some polynomial that has a root (y_0, z_0) modulo $(eM)^m$. Using the L^3-lattice basis reduction algorithm we then find a reduced basis $(v'_1, \ldots, v'_n)$ for $L(m,t)$. From Theorem 1, we know that

$$\|v'_1\| \leq \|v'_2\| \leq 2^{\frac{n}{4}} \det(L)^{\frac{1}{n-1}}.$$

To apply Howgrave-Graham's theorem, the second vector in the reduced basis must satisfy $\|v'_2\| < \frac{(eM)^m}{\sqrt{n}}$. A sufficient condition for this is

$$2^{\frac{n}{4}} \det(L)^{\frac{1}{n-1}} < \frac{(eM)^m}{\sqrt{n}},$$

which can be written as

$$\det(L) < 2^{-\frac{n(n-1)}{4}} n^{-\frac{n-1}{2}} (eM)^{m(n-1)}. \tag{11}$$

If (11) is satisfied, then the two polynomials whose coefficient vectors are v'_1 and v'_2 will each have (y_0, z_0) as a root over the integers. Computing the resultant of these two polynomials with respect to y will then yield a univariate polynomial in z with Λ as a root over the integers. Using standard root finding techniques we solve for Λ which then allows us to easily obtain the private key: Λ immediately yields $\phi(N)$, which allows us to compute $d = e^{-1} \bmod \phi(N)$.

Thus, we have an algorithm that takes (N, e), d_0, M, Y, Z, m, and t as input and outputs (N, d) if inequality (11) is satisfied. Again, since the bounds in Theorem 1 are not very tight the attack may still be successful even if (11) is not satisfied. As long as $\|v'_1\|$ and $\|v'_2\|$ are both less than $\frac{(eM)^m}{\sqrt{n}}$ the attack will work.

4.2 Multi-prime RSA

When extending this attack to multi-prime RSA, we obtain the following result.

Theorem 9. *Under Assumption 1, for every $\epsilon > 0$ and every integer $r \geq 2$ there exists an integer N_0 such that for every $N > N_0$ the following holds: Let (N, e) be an r-prime RSA public key with $\alpha = \log_N(e)$ is in the range*

$$0 < \alpha \leq \frac{4\,r - 1}{4\,r(r-1)}.$$

Given d_0 and δ_0 satisfying $d = d_0 \bmod N^{\delta_0}$ and

$$\delta_0 \geq \frac{1}{3} - \frac{1}{3\,r} + 2\,\frac{\sqrt{(r-1)(3\,\alpha\,r + r - 1)}}{3\,r} + \epsilon,$$

the private key (N, d) can be fully recovered in time polynomial in $\log N$.

For the first few values of r, plots showing the lower bound on the fraction of private exponent bits needed for all valid public exponents are shown in Figure 6. As can be seen, the bounds are similar to that of the attack in Section 3 except that the sufficient region is expanded for each r value. The trend of decreasing sufficient region continues for larger r values as well.

Partial Key Exposure Attack with known Least Significant Bits

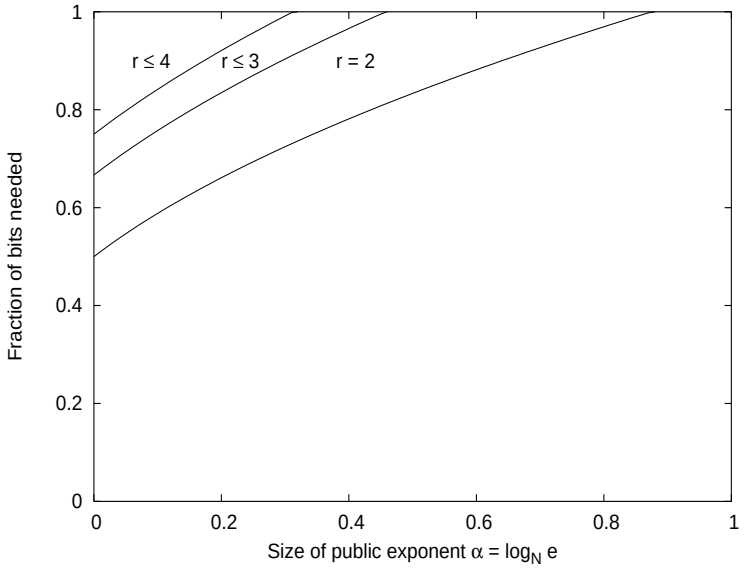


FIGURE 6: Lower bounds for δ

Proof (Theorem 9). Using the attack outlined in Section 4.1 we begin by letting $M = N^{\delta_0}$ and simplifying the bound for z_0 by $Z = N^{1-1/r}$. The simplification

of Z is allowed because $(2r-1)$ is negligible for fixed r and large N. Again, following Blömer and May, we introduce the parameter τ by letting $t = \tau\, m$ and rewrite everything in terms of m:

$$\begin{aligned} m(n-1) &= m^3\ (3\tau+2)(1+o(1))/2, \\ C_Y &= m^3(3\tau+2)(1+o(1))/6, \\ C_Z &= m^3(3\tau^2+3\tau+1)(1+o(1))/6, \\ C_{eM} &= m^3(3\tau+2)(1+o(1))/6. \end{aligned}$$

The determinant of the lattice (4.1) becomes

$$\det(L) = \left((eM)^{3\tau+2}\, Y^{3\tau+2} Z^{3\tau^2+3\tau+1}\right)^{\frac{1}{6}m^3(1+o(1))}.$$

Using the $Y = N^{\alpha}$, $Z = N^{1-1/r}$, and $eM = N^{\alpha+\delta_0}$ we then have

$$\det(L) = N^{\frac{1}{6}m^3\left(3(1-\frac{1}{r})\tau^2+3(1-\frac{1}{r}+2\alpha+\delta_0)\tau+1-\frac{1}{r}+4\alpha+2\delta_0\right)(1+o(1))},$$

and

$$(eM)^{m(n-1)} = N^{\frac{1}{2}m^3(\alpha+\delta_0)(2\tau+1)(1+o(1))}.$$

Neglecting all low order terms in m and terms that do not explicitly depend on N inequality (11) reduces to

$$3\left(1-\frac{1}{r}\right)\tau^2 + 3\left(1-\frac{1}{r}-\delta_0\right)\tau + 1 - \frac{1}{r} - \delta_0 + \alpha < 0. \tag{12}$$

Since $(1-1/r) > 0$ for all $r \geq 2$, the left hand side of (12) is minimized when

$$\tau = \frac{1}{2}\ \frac{\delta_0 - (1-\frac{1}{r})}{1-\frac{1}{r}}.$$

Upon substituting this value for τ into (12) we obtain

$$\left(-\frac{3}{2}\frac{1}{1-\frac{1}{r}}\right)\delta_0^2 + \delta_0 - \frac{3}{2}\frac{1}{1-\frac{1}{r}} + 2\left(1-\frac{1}{r}\right) + 2\alpha < 0.$$

Solving for δ_0 (and noting that the coefficient of δ_0^2 is always negative) we find that

$$\delta_0 > \frac{1}{3} - \frac{1}{3\,r} + 2\,\frac{\sqrt{(r-1)(3\,\alpha\,r+r-1)}}{3\,r}.$$

Finally, setting $\delta_0 = 1$ in (4.2) and solving for α yields

$$\alpha \leq \frac{4\,r-1}{4\,r(r-1)},$$

which concludes the proof. □

For the first few values of r, Table 4 shows bounds on δ_0 along with corresponding public exponent range. Again, letting $r = 2$ gives the same results that Blömer and May report for RSA.

r	$\alpha = \log_N(e)$	Fraction of bits needed
2	$[3, \frac{7}{8}]$	$\frac{1}{6} + \frac{1}{3}\sqrt{1+6\alpha}$
3	$[3, \frac{11}{24}]$	$\frac{2}{9} + \frac{2}{9}\sqrt{4+18\alpha}$
4	$[3, \frac{5}{16}]$	$\frac{1}{4} + \frac{1}{6}\sqrt{9+36\alpha}$

TABLE 4: For each r value and public exponent in the range given the last column gives the fraction of bits of the private exponent needed to guarantee success for the attack.

4.3 Experimental Results

As in Section 2.3, we present some experimental bounds on the fraction of bits of the private exponent needed to mount the attack for various modulus sizes and small lattice dimensions. Figure 7 shows the results for RSA with a 1024-bit modulus. For the smallest lattice dimensions considered, there seems to be a linear relationship with the fraction of bits needed and the size of the public exponent. As we increase the lattice dimension further, the attack maintains this linear behaviour for small public exponents but improves for larger public exponents. For these lattice dimension sizes ($n = 14, 18$), the actual attack covers an appreciable amount of the feasible region defined by the asymptotic bound.

Results for $r = 3$ with a 2048-bit modulus and $r = 4$ with a 4096-bit modulus are shown in Figure 8. Only the data for lattice dimensions 5 ($m = 1, t = 1$) and 25 ($m = 4, t = 2$) are shown. Experiments with dimensions $9, 12, 14$, and 18 resulted in essentially bounds within the uncertainty of the experiments. In all of these cases, the behaviour of the experimental bound was always found to be roughly linear the size of the public exponent. We suspect that for larger lattice dimensions, that the attack will become stronger for larger public exponents (as with $r = 2$), but we did not investigate that further. Nevertheless, the results show that even with small lattices the attack is quite effective with respect to the asymptotic sufficient conditions. The trend seems to indicate that the attacks approach the asymptotic bounds as r increases.

The results shown in Figures 7 and 8 are illustrative of all the experiments with this attack. As with the attack in Section 2, the results change very little with changing modulus size.

4.4 Algebraic Dependence

Let $p_1(y, z)$ and $p_2(y, z)$ denote the two polynomials corresponding to the first and second smallest vectors obtained from the lattice basis reduction, respectively, and let $p_{12} = \gcd(p_1, p_2)$ be the greatest common divisor of the two polynomials. In the vast majority of the experiments conducted for this at-

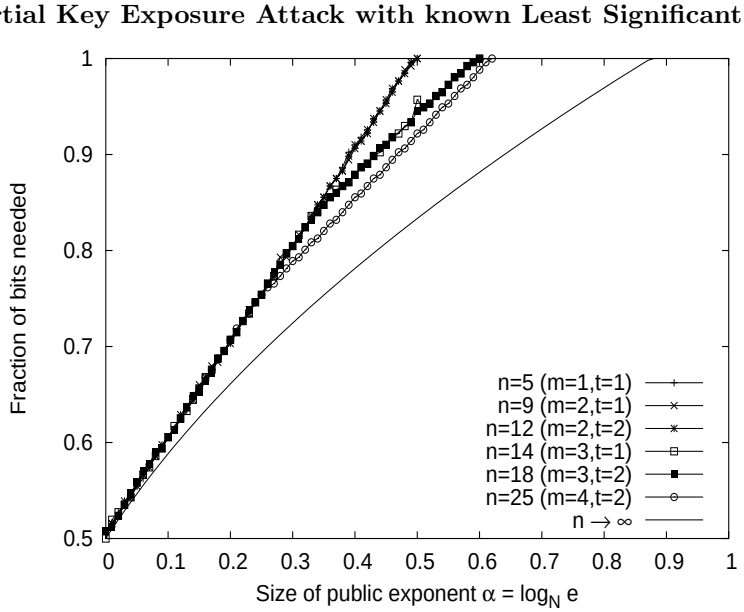
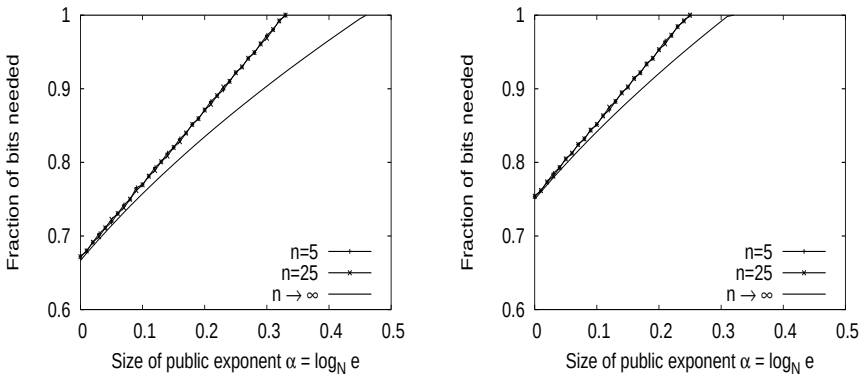


FIGURE 7: Experimental lower bounds of the fraction of MSBs required to attack RSA with a 1024-bit modulus.



(a) 2048-bit Modulus, $r = 3$ (b) 4096-bit Modulus, $r = 4$

FIGURE 8: Experimental lower bounds of the fraction of MSBs required to attack multi-prime RSA. (a) 3-prime RSA with 2048-bit modulus. (b) 4-prime RSA with 4096-bit modulus.

tack we have found that p_1 and p_2 were algebraically dependent (i.e., $p_{12} \neq 1$). Luckily enough though (from an attackers point of view), if we remove p_{12} from both p_1 and p_2 we always obtained two algebraically independent polynomials

that both have $(y, z) = (k, \Lambda)$ as a root over the integers. It is interesting that in all of these experiments we find that both p_1/p_{12} and p_2/p_{12} are of the form $a + by + cyz$, which reduced the time needed for the resultant computation since the degree of each polynomial is reduced. Unfortunately, this is not a general trend for larger lattice sizes. Mounting the attack for some larger dimension sizes ($m = 7, t = 1$, $m = 5, t = 1$, and others) for a given α and δ_0 that was successful for a smaller lattice we find that p_1 and p_2 are algebraically independent. This is consistent with the finding from [3].

4.5 Non-Asymptotic Bounds

As in Section 2.5, we find that the sufficient conditions for the attack computed for particular lattice parameters do not reflect the effectiveness of the actual attack. Figure 9 shows the sufficient condition to mount the attack against RSA with a 1024-bit modulus with a lattice of dimension 25 ($m = 4, t = 2$), the experimental lower bounds found, and the asymptotic sufficient conditions. Again, just as with the attack with known MSBs, the actual attack reflects the

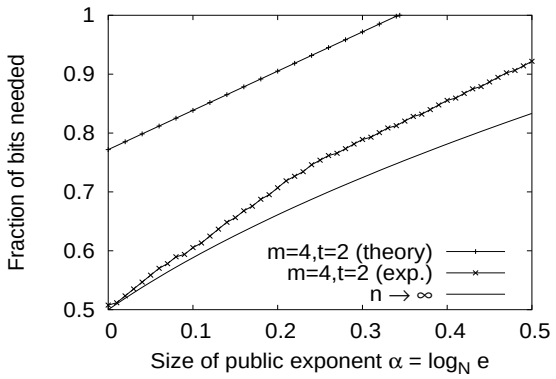


FIGURE 9: Lower bounds for LSBs. Comparison of theoretical and experimental results for RSA with 1024-bit modulus using lattice parameters $m = 4, t = 2$. The asymptotic theoretical sufficient condition is also shown.

asymptotic results much better than the non-asymptotic theoretical results.

5 Conclusions and Future Work

As with other attacks that have been extended to multi-prime RSA, see [5, 9] for example, the attacks in this work are weakened with each additional prime in the modulus. In particular, the sufficient region decreases with each additional prime: the range of public exponent decreases and the fraction of required bits of the private key increases.

An important factor to consider with respect to these partial key exposure attacks is which bits are potentially at risk. Whether an adversary can acquire the most significant or least significant bits, in a side channel attack say, depends on the particular algorithms used. For example, the simple square and multiply method of modular exponentiation can be done reading the exponents bits from left-to-right (potentially exposing the most significant bits of the exponent) or from right-to-left (potentially exposing the least significant bits of the exponent). By prescribing which algorithms to use, it is then possible to identify which type of attack is more feasible.

Below, we briefly discuss the algebraic dependence of the small vectors obtained from the LLL-algorithm in these attacks and compare the attacks with respect to the number of primes in the modulus.

5.1 Algebraic Dependence

The attacks in Sections 2 and 4 are both heuristic. This is because even if we find enough small vectors from the lattice basis reduction we cannot guarantee that we can find the desired small roots of their corresponding polynomials. Generally, it is heuristically assumed that the polynomials obtained in these types of applications are algebraically independent. In mounting these attacks, however, we have found that in many cases the polynomials obtained are algebraically dependent. But, as the experiments show, this property alone is not enough to defeat the attacks since we were able to find the desired roots by simply removing the common factors before computing the resultants. In fact, in all of the experiments that we carried out the attack very rarely failed because the polynomials were algebraically dependent. The attacks most often failed when the polynomials obtained did not have $\hat{\mathbf{x}}$ as a root over the integers (where $\hat{\mathbf{x}}$ is the desired small root) .

5.2 Most Significant Bits Known

Blömer and May's attack when extended to multi-prime RSA is very interesting in that the ranges of public exponents in which the attack can be mounted for different r values are disjoint in the asymptotic analysis. Even the experimental results show that the feasible regions in which that attack works only partially overlap. This is in contrast to all other attacks on RSA that have been extended to multi-prime RSA where the feasible region of attacking $(r+1)$-prime RSA is a strict subset of the feasible region of attacking r-prime RSA. However, when we combine all the known partial key exposure attacks with known MSBs together we find that this property (subsets of feasible regions) does indeed hold. Figure 10 shows the feasible region of all partial key exposure attacks on RSA and multi-prime RSA. The results for RSA are taken from Boneh, Durfee & Frankel [4] and Blömer & May [3]. The multi-prime RSA results come from Hinek, Low & Teske [9] and this work. From the experimental results obtained from these attacks, it seems that the theoretical (asymptotic) sufficient conditions are a good indication of the actual strength of the attacks.

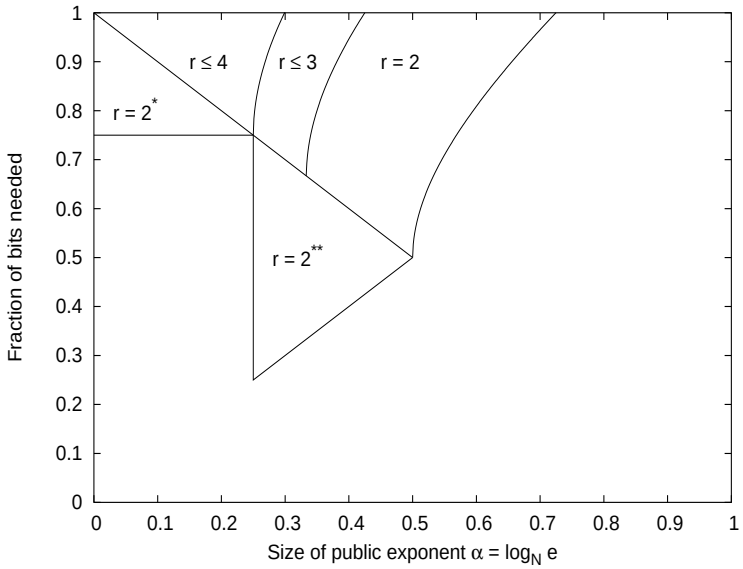


FIGURE 10: Feasible regions for all known partial key exposure attacks with known MSBs. ($\star$) it is not known if this attack, mentioned in [3], extends to multi-prime RSA. ($\star\star$) this attack, from [4] which requires that the factorization of e be known, does not extend to multi-prime RSA.

Accepting this, it is clear that using more primes in the modulus decreases the feasible region for these attacks. In particular, a user can safely use smaller public exponents with each additional prime in the modulus. Of course, simply using a public exponent $e \approx N$ will render all of these attacks useless.

5.3 Least Significant Bits Known

For the partial key exposure attacks with known LSBs we see that the feasible region for $(r+1)$-prime RSA is strict subset of the feasible region for r-prime RSA. The theoretical (asymptotic) sufficient conditions for all known attacks are shown in Figure 11. The attacks on RSA are from Boneh, Durfee & Frankel [4] and Blömer & May[3] while the multi-prime RSA attacks are from this work. As with the known MSB partial key exposure attacks, the experimental results for the partial key exposure attacks with known LSBs indicate that the theoretical (asymptotic) sufficient conditions needed to mount the attack are a good indication of the actual strength of the attacks. Again, accepting this, it clear that using more primes in the modulus decreases the feasible region of these attacks. In particular, a user can safely use smaller public exponents with each additional prime in the modulus. And, for public exponents that are vulnerable to the attacks, the fraction of bits needed for the attack seems to increase with

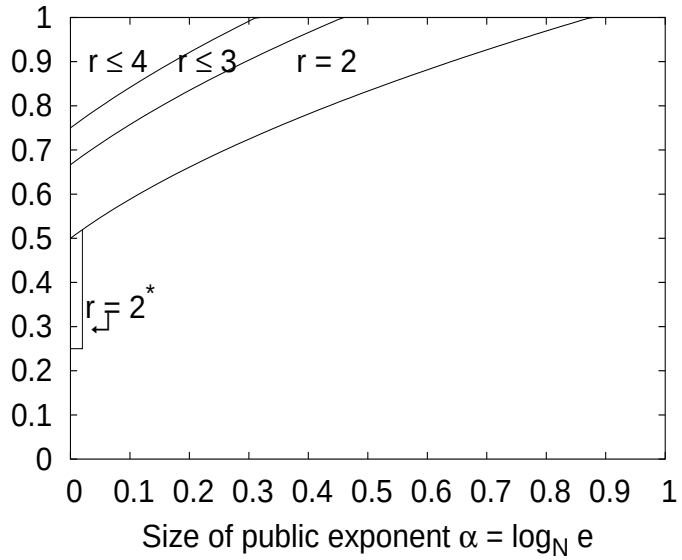


FIGURE 11: Feasible regions for all known partial key exposure attacks with known LSBs. ($\star$) this attack, from [4], does not extend to multi-prime RSA.

each additional prime. Of course, just as with the known MSBs attack, simply using a public exponent $e \approx N$ will render all of these attacks useless.

5.4 Future Work

More data should be gathered using larger lattice dimensions to give a clearer indication of how strong the attack actually is in practise. In particular, it would be interesting to see if the asymptotic bounds can be beaten in experiment and if so what lattice dimension is needed to do it.

Acknowledgements

The author would like to thank Alexander May for a helpful explanation of the small public exponent partial key exposure attack in which 3/4 of the MSBs of d are known.

References

[1] J. Blömer. Closest vectors, successive minima, and dual HKZ-bases of lattices. In *Proceedings of the 17th ICALP*, volume 1853 of *Lecture Notes in Computer Science*, pages 248–259. Springer, 2000.

[2] J. Blömer and A. May. Low secret exponent RSA revisited. In *Cryptography and Lattices – Proceedings of CALC '01*, volume 2146 of *Lecture Notes In Computer Science*, pages 4–19. Springer-Verlag, 2001.

[3] J. Blömer and A. May. New partial key exposure attacks on RSA. In *Advances in Cryptology - CRYPTO 2003*, volume 2729 of *Lecture Notes In Computer Science*, pages –. Springer-Verlag, 2003.

[4] D. Boneh, G. Durfee, and Y. Frankel. Exposing an RSA private key given a small fraction of its bits. Available for download at `http://crypto.stanford.edu/~dabo/abstracts/bits_of_d.html`. Revised and extended version version of the work from ASIACRYPT '98 - LNCS 1514.

[5] M. Ciet, F. Koeune, F. Laguillaumie, and J.-J. Quisquater. Short private exponent attacks on fast variants of rsa. UCL Crypto Group Technical Report Series CG-2003/4, Université Catholique de Louvain, 2003. Available at `http://www.dice.ucl.ac.be./crypto/tech_reports/CG2002_4.ps`.

[6] D. Coppersmith. Finding a small root of a bivariate integer equation; factoring with high bits known. In U. Maurer, editor, *Advances in Cryptology - EUROCRYPT '96*, volume 1070 of *Lecture Notes in Computer Science*, pages 178–189. Springer-Verlag, 1996.

[7] D. Coppersmith. Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *Journal of Cryptology*, 10(4):233–260, 1997.

[8] D. Coppersmith. Finding small solutions to small degree polynomials. In *Cryptography and Lattices – Proceedings of CALC '01*, volume 2146 of *Lecture Notes In Computer Science*. Springer-Verlag, 2001.

[9] M. J. Hinek, M. K. Low, and E. Teske. On some attacks on multi-prime rsa. In K. Nyberg and H. Heys, editors, *Selected Areas in Cryptography*, volume 2595 of *Lecture Notes in Computer Science*, pages 385–404. Springer-Verlag, 2003.

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

[11] A. K. Lenstra. Unbelievable security : Matching AES security using public key systems. In *Advances in Cryptology - ASIACRYPT 2001*, volume 2248 of *Lecture Notes In Computer Science*, pages 67–86. Springer-Verlag, 2001.

[12] A. K. Lenstra, H. W. Lenstra, and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261:515–534, 1982.

[13] Maplesoft. Maple 9. Information available at `http://www.maplesoft.com`.

[14] J. Proos. *Imperfect Decryption and Partial Information Attacks in Cryptography*. PhD thesis, University of Waterloo, 2003.

[15] V. Shoup. NTL: A library for doing number theory, version 5.3.1. Available online at `http://shoup.net/ntl/`.