

On the Security of Multi-prime RSA

M. Jason Hinek

David R. Cheriton School of Computer Science
University of Waterloo
Waterloo, Ontario, N2L 3G1, Canada
mjhinek@alumni.uwaterloo.ca

June 13, 2006

Abstract. In this work we collect the strongest known algebraic attacks on multi-prime RSA. These include factoring, small private exponent, small CRT exponent and partial key exposure attacks. Five of the attacks are new. A new variant of partial key exposure attacks is also introduced which applies only to multi-prime RSA with more than two primes.

1 Introduction

The RSA cryptosystem, invented by Rivest, Shamir and Adleman [23], is the most widely known and widely used public key cryptosystem in the world today. The main drawback of using RSA, however, is the relatively costly encryption and decryption operations. Multi-prime RSA is a generalization of the standard RSA cryptosystem in which the modulus contains more than two primes. When decryption operations are done modulo each prime and then combined using the Chinese Remainder Theorem, the cost of decryption is reduced with each additional prime added to the modulus (for a fixed modulus size). Thus, multi-prime RSA might be a practical alternative to RSA when decryption costs need to be lowered. The security of RSA has been well studied (see Boneh [3]) since it was invented. If multi-prime RSA is to be actually implemented and used, its security must be investigated further.

The aim of this work is to present the current state of security of multi-prime RSA with respect to algebraic attacks. In particular, we collect the best known attacks on multi-prime RSA as well as introduce several new attacks. While the primary focus is on multi-prime RSA with more than two primes in the modulus, we also include the best known attacks on RSA to give a more complete analysis.

The rest of this paper is organized as follows. The remainder of this section introduces some notation and assumptions concerning multi-prime RSA, and reviews some results for finding small solutions of multivariate polynomials. The next six sections present all of the attacks that we consider in this work. In particular, Section 2

presents factoring attacks which apply to any integers having the same form as multi-prime moduli. Section 3 considers the small private exponent attacks derived from Wiener’s and Boneh and Durfee’s attacks. In sections 4 and 5, we consider partial key exposure attacks in which some of the bits of the private exponent are known. We present three new attacks which are extensions of the partial key exposure attacks of Ersnt et al. [14]. Two of the attacks require some of the most significant bits of the private exponent and one requires some of the least significant bits. In Section 6, we consider partial key exposure attacks in which some of the bits of the primes in the modulus are known and, in addition, some of the bits of the private exponent are known. Two new attacks are introduced here. The first is a factoring attack which applies to integers of the same form as multi-prime RSA moduli with known partial factorization. This attack is a generalization of Boneh, Durfee and Howgrave-Graham’s lattice-based factoring method for moduli of the form $N = p^r q$. The second is an attack on small private exponent multi-prime RSA in which some of the most significant bits of the private exponent and some of the bits of the primes in the modulus are known. Section 7 finishes the collection of attacks with an attack on multi-prime RSA which uses the Chinese Remainder Theorem for decryption and small CRT exponents. Experimental data illustrating the practical effectiveness of some of the attacks from Sections 3–5 is presented in Section 8. We conclude with some final remarks in Section 9.

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, \dots, 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 $ed \equiv 1 \pmod{\phi(N)}$ (i.e., compute $d = e^{-1} \pmod{\phi(N)}$). The private key is the pair (N, d) .

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

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

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 $\frac{3}{2^{r-3}}(\log_2 N)^3$ (using standard arithmetic). 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. As we shall see in Section 2, using too many primes in the modulus increases the risk of the modulus being factored. Thus, a trade-off is analyzed.

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

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

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 congruence $ed \equiv 1 \pmod{\phi(N)}$ is called the the public/private key relation, or simply the key relation. Writing this congruence as an equation yields

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

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

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

As shown in [18], a simple computation using the above expression for Λ and (1) shows that Λ satisfies

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

Thus, $\phi(N)$ and N have roughly an $(r - 1)/r$ fraction of their most significant bits in common.

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 β or δ to denote the size of the private exponent ($d = N^\beta$ or $d = N^\delta$) depending on the context. Also, we often use the acronyms MSB and LSB as shorthand for most significant bits and least significant bits, respectively.

1.2 Small Solutions of Polynomials

Here we collect some results concerning finding small solutions to polynomials. The results are all based on Coppersmith’s techniques for finding small solutions to polynomials and will only be used as tools to prove some of the results found later in this work. For more information about Coppersmith’s techniques, we refer the reader to Coppersmith’s original papers [10,11,12], Howgrave-Graham’s simplification of the univariate modular case [19] and Coron’s simplification of the bivariate case [13]. In addition to these provable results, there are many heuristic extensions of Coppersmith’s techniques to multivariate modular polynomials (see Boneh and Durfee [4] for example) and multivariate integer polynomials with more than two variables (see Ernst et al. [14] for a recent example). All of the heuristic extensions rely on the assumption that the first few small polynomials obtained by lattice basis reduction are algebraically independent (which allows a system of polynomials to be solved over \mathbb{Z}). While it is often claimed that this assumption is valid in practice, there have been reports that when the bounds are near the limiting values the assumption begins to fail (see Hinek[17, §6.1] for example). We will use the term “Coppersmith’s techniques” to refer to the original techniques as well any of the extensions.

The first result is essentially Coppersmith’s original univariate modular result given in its most general form (as stated by May [22]). A proof can be found in [15, §3.1].

Theorem 1. *Let N be an integer of unknown factorization, which has a divisor $b \geq N^\beta$. Let $f_b(x)$ be a monic univariate polynomial of degree d , let c_N be a function that is upper-bounded by a polynomial in $\log N$, and let $\epsilon > 0$. Then, for sufficiently large N , we can find all solutions x_0 for the equation $f_b(x) \equiv 0 \pmod{b}$ such that*

$$|x_0| \leq c_N N^{\beta^2/d-\epsilon},$$

in time polynomial in $\log N$, $1/\epsilon$ and linear in the number of solutions.

The next two results are generalizations of Coppersmith's method for bivariate integer polynomials by Ernst et al. [14]. Both results are heuristic and rely on the following assumption:

Algebraic Independence Assumption *The small (normed) polynomials found by lattice basis reduction in the methods implicit in Coppersmith's techniques are algebraically independent.*

We restate the results in terms of general polynomials. In the following, let $X = N^{\eta_x}$, $Y = N^{\eta_y}$ and $Z = N^{\eta_z}$ for some integer N and real positive η_x , η_y , and η_z . Also, we use $\|f\|_\infty$ to denote the largest coefficient, in absolute value, of all monomials in the polynomial f .

Theorem 2. *Consider the polynomial*

$$f_1(x, y, z) = c_x x + c_y y + c_{yz} yz + c_1 \in \mathbb{Z}[x, y, z].$$

For any $\hat{\epsilon} > 0$, all roots (x_0, y_0, z_0) satisfying $|x_0| < X$, $|y_0| < Y$ and $|z_0| < Z$ for some bounds X , Y and Z can be found if N is sufficiently large and

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

for some $\tau \geq 0$, provided that algebraic independence assumption holds, where $W = \|f_1(xX, yY, zZ)\|_\infty$. Further, the roots can be found in time polynomial in $\log N$ and $1/\hat{\epsilon}$ and linear in the number of solutions.

Theorem 3. *Consider the polynomial*

$$f_2(x, y, z) = c_x x + c_y y + c_{yz} yz + c_z z + c_1 \in \mathbb{Z}[x, y, z].$$

For any $\hat{\epsilon} > 0$, all roots (x_0, y_0, z_0) satisfying $|x_0| < X$, $|y_0| < Y$ and $|z_0| < Z$ for some bounds X , Y and Z can be found if N is sufficiently large and

$$X^{2+3\tau} Y^{3+6\tau+3\tau^2} Z^{3+3\tau} \leq W^{2+3\tau-\hat{\epsilon}},$$

for some $\tau \geq 0$, provided that algebraic independence assumption holds, where $W = \|f_2(xX, yY, zZ)\|_\infty$. Further, the roots can be found in time polynomial in $\log N$ and $1/\hat{\epsilon}$ and linear in the number of solutions.

For a proof of these results, see Ernst et al. [14].

2 Factoring Attacks

The best generic factoring method is the general number field sieve (NFS). Following Lenstra [20], we will use

$$L[N] = e^{1.923(\log N)^{1/3}(\log \log N)^{2/3}}, \quad (2)$$

as the heuristic expected runtime of the NFS to compute a non-trivial factor of the composite number N . Notice that the runtime depends only on the bitsize of the integer to be factored. Thus, when using the NFS, it is expected that the time needed to factor an n -bit RSA modulus will be the same as that needed to factor an n -bit r -prime RSA modulus for any $r > 2$. For RSA ($r = 2$) with balanced primes, the NFS is the best factoring method. The largest RSA modulus factored, as of May 2005 [27], is RSA200, a 200-digit (665-bit) modulus. This is also the largest composite integer, in general, that has been factored with the NFS.

The elliptic curve method (ECM) for factoring can compute a non-trivial factor p of a composite integer N substantially faster than the NFS if the factor is significantly smaller than \sqrt{N} . Again, following Lenstra [20], we use

$$E[N, p] = (\log_2 N)^2 e^{\sqrt{2}(\log p)^{1/2}(\log \log p)^{1/2}}, \quad (3)$$

as the heuristic expected runtime of the ECM to find a factor p of N . Notice that the runtime is sub-exponential in the bitsize of the factor p and polynomial in the bitsize of the integer to be factored. Thus, when using the ECM, it is expected that the time needed to factor an n -bit RSA modulus with balanced primes will be greater than that needed to factor an n -bit r -prime RSA modulus with balanced primes for any $r > 2$ (since the prime factors are smaller). Further, the runtime decreases with increasing number of primes. The largest factor found with the ECM, as of April 2005 [27], is 66 digits (220 bits).

The security of RSA is usually estimated by the difficulty of factoring the modulus. For example, the estimated time complexity to factor a 1024-bit RSA modulus with balanced primes is roughly 2^{80} (using the NFS). Thus, RSA with a 1024-bit modulus offers roughly the same security as an 80-bit one time pad. For multi-prime RSA, the security is still estimated by the difficulty of factoring the modulus. However, for a given modulus size, the security of r -prime RSA with balanced primes should be no less than the security of RSA with the same modulus size. Thus, the number of primes in the modulus must be small enough so that the expected complexity of the ECM is not less than the expected complexity of the NFS. Any value of r that satisfies this is considered a “safe” value.

Table 1 lists the estimated maximum number of balanced primes that are considered safe for various modulus sizes. The data in the table is taken from [9], and was determined by the crossover point of the expected runtimes of the NFS and ECM.

Modulus size (bits)	1024	2048	4096	8192
Maximum number of primes (r)	3	3	4	5

Table 1. Estimated maximum number of safe primes allowed for various modulus sizes.

Therefore, for a given modulus size, the security of r -prime RSA with balanced primes is the same for all safe values of r . Once the number of primes is increased beyond the maximum number given in Table 1, however, the security is decreased. In fact, once the number of primes is no longer a safe number, the security decreases with each additional prime in the modulus. From the perspective of the attack (i.e., factoring algorithms), the strength of the attack increases with increasing number of primes in the modulus. As we shall see in the remainder of this work, this correspondence of attack strength with number of primes is unique. In all other attacks that have been mounted on RSA and r -prime RSA, for $r > 2$, the attacks decrease in strength with each additional prime in the modulus.

3 Small Private Exponent Attacks

In this section we consider the small private exponent attacks on RSA and their extensions to multi-prime RSA. Given only the public key these attacks will recover the private exponent provided it is sufficiently small. We consider three attacks in this section: Wiener’s continued fraction attack, Boneh and Durfee’s lattice-based attack and Blömer and May’s lattice-based attack.

The first significant small private exponent attack on RSA was Wiener’s continued fraction attack [26]. Using the convergents of the continued fraction expansion of e/N , Wiener is able to recover the private exponent if it is sufficiently small. The attack was extended to multi-prime RSA by Hinek, Low and Teske [18] and also by Ciet et al. [8]. The result of the attack on multi-prime RSA, [18, Theorem 2], is given below.

Attack 1 *For every integer $r \geq 2$ the following holds: Let N be an r -prime RSA modulus with balanced primes. Given a valid public key (N, e) with corresponding*

private key (N, d) , if

$$d < \frac{N^{1/(2r)}}{\sqrt{2(2r-1)}},$$

then the private exponent can be computed in time polynomial in $\log N$.

Letting $r = 2$ recovers the condition $d < N^{1/4}/\sqrt{6}$, obtained by Boneh [3], which is the same as Wiener's original result [26] up to a multiplicative constant. A proof of Attack 1 can be found in [18, §4.1].

The next significant attacks on small private exponent RSA were by Boneh and Durfee [4]. Based on Coppersmith's method for finding small solutions of univariate modular equations, Boneh and Durfee present two attacks which increase the range of small private exponents that are insecure. Unlike Wiener's attack, however, the lattice-based attacks are only heuristic and the bounds obtained are for the limiting case of large RSA moduli and large lattice dimension. The attacks do work well in practice though.

Boneh and Durfee's strongest lattice-based attack uses sublattices and introduces geometrically progressive matrices to give bounds on the volume of the sublattices used. Before giving the multi-prime extension of this attack, we first consider a simpler approach to using sublattices which was given by Blömer and May [1]. The bound obtained by Blömer and May gives the second strongest attack against small private exponent RSA. Their result was extended to multi-prime RSA (as well as arbitrary public exponent) by Hinek, Low and Teske [18, equation 18]. The result is as follows¹.

Attack 2 *For every $\epsilon > 0$ and integer $r \geq 2$ there exists an N_0 such that, for every $N > N_0$, the following holds: Let N be an r -prime RSA modulus with balanced primes, let (N, e) be a valid public key and let (N, d) be its corresponding private key, where $e = N^\alpha$ and $d = N^\delta$. Given (N, e) , if the private exponent satisfies*

$$\delta \leq \frac{6}{5r} - \frac{1}{5} - \frac{3\alpha}{5} + \frac{2}{5r} \sqrt{\alpha^2 r^2 - \alpha r(r-1) + 4(r-2)^2} - \epsilon,$$

then d can be recovered in time polynomial in $\log N$ and $1/\epsilon$, provided the algebraic independence assumption holds.

Letting $r = 2$ and $\alpha = 1$ recovers the bound $\delta < (\sqrt{6} - 1)/5 \approx 0.290$, originally obtained by Blömer and May [1, §4]. A proof of the result in Attack 2 can be found in [18, §4.2].

¹ Hinek, Low and Teske use the variable $a_r = (1-r)/r$ to simplify their presentation.

We end this section with an extension of the strongest of Boneh and Durfee’s lattice-based attacks. This attack gives the best theoretical bound for small private exponents that are insecure. The attack was extended to multi-prime RSA by Ciet et al. [8]. The result of this extension, using the approximation $\alpha \approx 1$, is as follows.

Attack 3 *For every $\epsilon > 0$ and integer $r \geq 2$ there exists an N_0 such that for every $N > N_0$ the following holds: Let N be an r -prime RSA modulus with balanced primes, let (N, e) be a valid public key and let (N, d) be its corresponding private key, where $e = N^\alpha$ and $d = N^\delta$. Given (N, e) , if $\alpha \approx 1$ and the private exponent satisfies*

$$\delta \leq 1 - \sqrt{1 - \frac{1}{r}} - \epsilon,$$

then d can be recovered in time polynomial in $\log N$ and $1/\epsilon$, provided the algebraic independence assumption holds.

Letting $r = 2$ recovers the bound $\delta \leq 1 - \sqrt{1/2} \approx 0.292$, originally obtained by Boneh and Durfee [4, §5]. A proof of the result in Attack 3 can be found in [8, §4.2.1].

4 Partial Key Exposure Attacks: Known MSB

In this section we assume that the adversary has an approximation to the high order bits of the private exponent $d = N^\beta$. That is, for a given public key (N, e) , the adversary knows \hat{d} such that $|d - \hat{d}| < N^\delta$ for some $0 \leq \delta \leq \beta$.

The two main lattice-based results for known partial key exposure attacks on RSA when either the public or private exponent is small are by Ernst, Jochemsz, May and de Weger [14]. We extend their results here to obtain new attacks on multi-prime RSA. The first attack uses the key equation with the approximation \hat{d} to compute d . We have the following new attack.

Attack 4 *For every $\epsilon > 0$ and integer $r \geq 2$ there exists an N_0 such that for every $N > N_0$ the following holds: Let N be an r -prime RSA modulus with balanced primes, let (N, e) be a valid public key and let (N, d) be its corresponding private key, where $e = N^\alpha$ and $d = N^\beta$. Given the public key (N, e) and \hat{d} satisfying $|d - \hat{d}| \leq N^\delta$, if*

$$\delta \leq \frac{2}{3} + \frac{1}{3r} - \frac{2}{3r} \sqrt{(r-1)(3\alpha r + 3\beta r - 2r - 1)} - \epsilon \quad (4)$$

then d can be recovered in time polynomial in $\log N$ and $1/\epsilon$, provided the algebraic independence assumption holds.

Proof: Starting with the key equation $ed = 1 + k\phi(N)$, we replace d with $\widehat{d} + d_0$ and $\phi(N)$ with $N - \Lambda$, to obtain

$$e(\widehat{d} + d_0) = 1 + k(N - \Lambda).$$

Here d_0 , k and Λ are the only unknowns. Replacing each of these unknowns with a variable leads to the following polynomial:

$$f(x, y, z) = ex - Ny + yz + (e\widehat{d} - 1) \in \mathbb{Z}[x, y, z],$$

which by construction has the integer root $(x_0, y_0, z_0) = (d_0, k, \Lambda)$. Let X , Y and Z be bounds for $|x_0|$, $|y_0|$ and $|z_0|$, respectively, defined by

$$\begin{aligned} |x_0| &= |d_0| < N^\delta = X, \\ |y_0| &= |k| = \left\lfloor \frac{ed-1}{\phi(N)} \right\rfloor < 2N^{\alpha+\beta-1} = Y, \\ |z_0| &= |\Lambda| < (2r-1)N^{1-1/r} = Z, \end{aligned}$$

and let $W = \|f(xX, yY, zX)\|_\infty$. Since $f(x, y, z)$ has the same set of monomials as the polynomial in Theorem 2, it follows that, for any $\hat{\epsilon} > 0$ and $\tau \geq 0$, we can compute (x_0, y_0, z_0) if N is sufficiently large and

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

provided that the algebraic independence assumption holds. Substituting $X = N^\delta$, $Y = N^{\alpha+\beta-1}$, $Z = 3N^{1-1/r}$ and $W = \max(eX, NY, YZ, e\widehat{d} - 1) = NY = 2N^{\alpha+\beta}$, this inequality reduces to

$$(r-1)\tau^2 + (\delta r - 1)\tau + \frac{1}{3}(\delta r + \alpha r + \beta r - r - 1) \leq 0,$$

in the limiting case of $N \rightarrow \infty$, if we let all lower order terms and factors independent of N be absorbed into $\hat{\epsilon}$. We can minimize the left-hand side of this inequality for any choice of α , δ and $r \geq 2$ by letting $\tau = -\frac{1}{2}(\delta r - 1)/(r - 1)$. Using this value for τ and solving for δ , we find that

$$\delta \leq \frac{2}{3} + \frac{1}{3r} - \frac{2}{3r} \sqrt{(r-1)(3\alpha r + 3\beta r - 2r - 1)},$$

is a sufficient condition to recover the root (x_0, y_0, z_0) using the method implicit in Theorem 2. \square

The second attack uses the partial knowledge of the private exponent to compute an approximation of the constant k in the key equation. In some instances (i.e., for particular sizes of public and private exponents), using the approximations of both d and k improve the result of the previous attack. We have the following new attack.

Attack 5 For every $\epsilon > 0$ and integer $r \geq 2$ there exists an N_0 such that for every $N > N_0$ the following holds: Let N be an r -prime RSA modulus with balanced primes, let (N, e) be a valid public key and let (N, d) be its corresponding private key, where $e = N^\alpha$ and $d = N^\beta$. Given the public key (N, e) and \widehat{d} satisfying $|d - \widehat{d}| \leq N^\delta$, if

1. $\alpha > 1 - \delta$, $\delta \leq \beta - 1/r$ and

$$\delta \leq \frac{3r^2 + 6\alpha r + 3 - r^2\alpha^2 - 6r - 2\alpha r^2}{4\alpha r^2} - \epsilon, \text{ or} \quad (5)$$

2. $\alpha > 1 + 1/r - \beta$, $\delta \geq \beta - 1/r$ and

$$\delta \leq \frac{\alpha + \beta - 1}{3} + \frac{2}{3r} - \frac{2}{3r} \sqrt{(\alpha r + \beta r - r - 1)(\alpha r + \beta r + 2r - 4)} - \epsilon, \quad (6)$$

then d can be recovered in time polynomial in $\log N$ and $1/\epsilon$, provided the algebraic independence assumption holds.

Proof: First we use N , e and \widehat{d} to compute an approximation \widehat{k} of the constant k in the key equation. Let

$$\widehat{k} = \left\lfloor \frac{e\widehat{d} - 1}{N} \right\rfloor. \quad (7)$$

It follows that \widehat{k} is a good approximation of the high bits of k . In fact, we have that (see [16, §2.2] for the first inequality)

$$\left| \widehat{k} - k \right| \leq \frac{e}{\phi(N)} \left(N^\delta + (2r - 1)\widehat{d}N^{-1/r} \right) \leq 2rN^\gamma, \quad (8)$$

where $\gamma = \max(\alpha + \delta - 1, \alpha + \beta - 1 - \frac{1}{r})$. Using this approximation for k we can then write the key equation as

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

where $d_0 = d - \widehat{d}$, $k_0 = k - \widehat{k}$ and Λ are the only unknowns. Replacing each of the unknowns with a variable leads to the following polynomial:

$$g(x, y, z) = ex - yN + \widehat{k}z + yz + e\widehat{d} - 1 - \widehat{k}N \in \mathbb{Z}[x, y, z],$$

which by construction has the integer root $(x_0, y_0, z_0) = (d_0, k_0, \Lambda)$. Let X , Y and Z be bounds for $|x_0|$, $|y_0|$ and $|z_0|$, respectively, defined by

$$\begin{aligned}
|x_0| &= |d_0| < N^\delta = X, \\
|y_0| &= |k_0| < 2rN^\gamma = Y, \\
|z_0| &= |A| < (2r-1)N^{1-1/r} = Z,
\end{aligned}$$

and let $W = \|g(xX, yY, zX)\|_\infty$. Since $g(x, y, z)$ has the same set of monomials as the polynomial in Theorem 3, for any $\hat{\epsilon} > 0$ and $\tau \geq 0$ we can compute (x_0, y_0, z_0) if N is sufficiently large and

$$X^{2+3\tau}Y^{3+6\tau+3\tau^2}Z^{3+3\tau} \leq W^{2+3\tau-\hat{\epsilon}}, \quad (9)$$

provided that the algebraic independence assumption holds. Using $X = N^\delta$, $Y = 2rN^\gamma$, $Z = 3N^{1-1/r}$ and $W = \max(eX, NY, \hat{k}Z, YZ, e\hat{d} - 1 - \hat{k}N) = NY = 2rN^{\gamma+1}$, inequality (9) reduces to

$$(\gamma r)\tau^2 + (\gamma r + \delta r - 1)\tau + \frac{1}{3}(2\delta r + r - 3 + \gamma r) < 0,$$

in the limiting case of $N \rightarrow \infty$, if we let all lower order terms and factors independent of N be absorbed into $\hat{\epsilon}$.

When $\gamma > 0$, we can minimize the left-hand side of this inequality for any choice of α , δ and $r \geq 2$ by letting $\tau = -\frac{1}{2}(\gamma r + \delta r - 1)/(\gamma r)$. Using this value for τ and solving for δ , we find that

$$\delta \leq \frac{\gamma}{3} + \frac{1}{r} - \frac{2}{3r}\sqrt{\gamma^2 r^2 - 3\gamma r + 3\gamma r^2}, \quad (10)$$

is a sufficient condition to recover the root (x_0, y_0, z_0) using method implicit in Theorem 3.

We now consider the two cases for γ separately. That is, we consider $\gamma = \alpha + \delta - 1$ and $\gamma = \alpha + \beta - 1 - 1/r$. The cases can be distinguished by the values of δ and $\beta - 1/r$ (the cases overlap when $\delta = \beta - 1/r$). For each case, we must ensure that $\gamma > 0$ so that the optimization of τ given above holds.

1. When $\delta \leq \beta - 1/r$ and hence $\gamma = \alpha + \delta - 1$, inequality (10) becomes

$$\delta \leq \frac{3r^2 + 6\alpha r + 3 - r^2\alpha^2 - 6r - 2\alpha r^2}{4\alpha r^2}. \quad (11)$$

For this case, in order to ensure $\gamma > 0$ we must have $\alpha > 1 - \delta$.

2. When $\delta \geq \beta - 1/r$ and hence $\gamma = \alpha + \beta - 1 - 1/r$, inequality (10) becomes

$$\delta \leq \frac{\alpha + \beta - 1}{3} + \frac{2}{3r} - \frac{2}{3r} \sqrt{(\alpha r + \beta r - r - 1)(\alpha r + \beta r + 2r - 4)} - \epsilon, \quad (12)$$

In order to ensure that $\gamma = \alpha + \beta - 1 - 1/r > 0$, we must have that $\alpha > 1 + 1/r - \beta$ in this case.

This completes the proof. \square

While it is possible to have public and private exponents both significantly smaller than $\phi(N)$ (see Sun and Yang [25] for example), it is much more common that only one of the exponents is small. We consider the strongest attacks for these typical instances, when only one exponent is small, below. The attacks are summarized in Figure 1 for the first few values of r . Notice that the effectiveness of each attack decreases with each additional prime in the modulus.

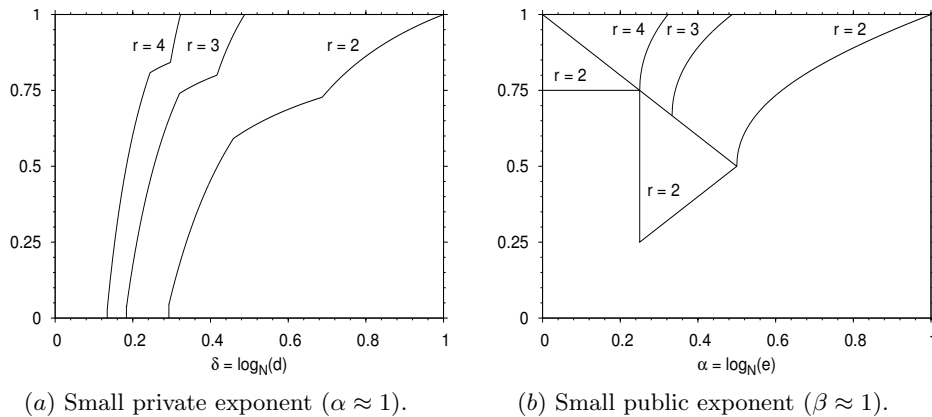


Fig. 1. Partial key exposure attacks with known MSB and small private exponent.

4.1 Small Private Exponent

In typical RSA, when the private exponent is chosen to be small, the public exponent is roughly the same order of magnitude as the modulus N . Thus, in this scenario we can approximate the public exponent by $e \approx N$ (i.e., $\alpha \approx 1$). Using this approximation in Attack 4, we have that for sufficiently large N the private exponent can be computed if

$$\delta \leq \frac{2}{3} + \frac{1}{3r} - \frac{2}{3r} \sqrt{(r-1)(r+3\beta r-1)} - \epsilon, \quad (13)$$

Similarly, in Attack 5, we have that for sufficiently large N the private exponent can be computed if

$$\delta \leq \frac{3}{4r^2} - \epsilon, \quad (14)$$

when $\beta \leq (3 + 4r)/(4r^2)$, or if

$$\delta \leq \frac{\beta}{3} + \frac{2}{3r} - \frac{2}{3}\sqrt{(r\beta - 1)(r\beta - 4 + 3r)} - \epsilon, \quad (15)$$

when $\beta \geq (3 + 4r)/(4r^2)$. Since $\alpha \approx 1$, we have $\gamma > 0$ for both cases. Letting $r = 2$ in the preceding three equations recovers the original results for RSA by Ernst et al. [14, Theorem 1]. In particular, when $r = 2$, the private exponent can be recovered if:

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

In addition to Attacks 4 and 5, both of the small private exponent attacks (Wiener; Boneh and Durfee) can be considered as partial key exposure attacks with known MSB and small private exponent. In this case, zero bits of the private key are required to successfully mount the attack (i.e., $\delta = 0$).

We illustrate the partial key exposure attacks with small private exponent for the first few values of r when $\alpha \approx 1$ in Figure 1(a). For each value of β , the fraction of bits of the private exponent required for the attack to succeed is given (i.e., $(\beta - \delta)/\beta$). For each value of r , Attack 3 is strongest for small β , Attack 4 is strongest for intermediate values of β and Attack 5 is strongest for larger values of β .

4.2 Small Public Exponent

In typical RSA, when the public exponent is chosen to be small, the private exponent is roughly the same order as magnitude as the modulus N . Thus, in this scenario we can approximate the private exponent by $d \approx N$ (i.e., $\beta \approx 1$). Using this approximation in Attack 5, we have that for sufficiently large N the private exponent can be computed when $e > N^{1/r}$ ($\alpha > 1/r$ to ensure $\gamma > 0$) and

$$\delta \leq \frac{\alpha}{3} + \frac{2}{3r} - \frac{2}{3r}\sqrt{(\alpha r - 1)(\alpha r + 3r - 4)} - \epsilon. \quad (16)$$

Letting $r = 2$ recovers the original RSA result obtained by Ernst et al. [14, Theorem 2]. Namely, $\delta \leq \frac{1}{3} + \frac{1}{3}\alpha - \frac{1}{3}\sqrt{4\alpha^2 + 2\alpha - 2} - \epsilon$.

When the public exponent is smaller than $N^{1/r}$, an attack that is not based on lattice basis reduction can be used. The original attack on RSA is by Boneh, Durfee and Frankel [6] and was extended to the multi-prime case by Hinek, Low and Teske [18]. The main result of the attack follows.

Attack 6 *For every integer $r \geq 2$ there exists an N_0 such that for every $N > N_0$ the following holds: Let N be an r -prime RSA modulus with balanced primes, let (N, e) be a valid public exponent and let (N, d) be its corresponding private key, where $e \leq N^{1/r}$ and $k = (ed - 1)/\phi(N) > \eta e$ for some $0 < \eta < 1$. Given (N, e) and an approximation \widehat{d} of d satisfying $|d - \widehat{d}| < e$, the private exponent can be computed in time polynomial in r , $\log N$ and $1/\eta$.*

For a proof of Attack 6, see [18, §5.2].

In Figure 1(b), we illustrate the partial key exposure attacks with small public exponent for the first few values of r when $\beta \approx 1$. For each value of α , the fraction of bits of the private exponent required for the attack to succeed is given (i.e., $1 - \delta$). In addition to Attacks 5 and 6, we have included two additional partial key exposure attacks by Boneh, Durfee and Frankel [6] that only apply to RSA. We include these attacks to give a complete picture of the best partial key exposure attacks on multi-prime RSA (including RSA). We give the results of these attacks below. For arguments that these attacks cannot be extended to the multi-prime case, see Hinek, Low and Teske [18, §5.2].

The first attack yields applies to instances of RSA with public exponent in the range $1/4 \leq \alpha \leq 1/2$. It is the strongest known partial key exposure attack with known MSB against RSA, occurring when $e \approx N^{1/4}$. The main result of the attack follows (see [6, Theorem 4.3] for more details including a proof of the result).

Attack 7 *For every $\epsilon > 0$ there exists an N_0 such that for every $N > N_0$ the following holds: Let N be an RSA modulus with balanced primes, let (N, e) be a valid public key with prime public exponent and let (N, d) be its corresponding private key, where $e = N^\alpha$. Given (N, e) where $\frac{1}{4} \leq \alpha \leq \frac{1}{2}$ and \widehat{d} satisfying $|d - \widehat{d}| < N^{\alpha - \epsilon}$, the private exponent can be computed in time polynomial in $\log N$ and $1/\epsilon$.*

This attack requires that the public exponent be prime. If e is not prime, the attack can still be mounted provided that the factorization of e is known. If e has t distinct prime factors then the runtime of the modified attack is polynomial in $\log N$, $1/\epsilon$ and

2^t . For details, see [6, Corollary 4.4]. For a 1024-bit modulus and randomly chosen $e < N^{1/2}$, it should be possible to completely factor e using the ECM (see Section 2).

The second attack, observed by Blömer and May [2, §1], is not explicitly mentioned by Boneh, Durfee and Frankel but follows from two of their results [6, Theorems 3.3 and 4.1]. The main result of the attack, which applies to instances of RSA with public exponent smaller than $N^{1/4}$, is as follows.

Attack 8 *For every $\epsilon > 0$ there exists an N_0 such that for every $N > N_0$ the following holds: Let N be an RSA modulus with balanced primes, let (N, e) be a valid public key and let (N, d) be its corresponding private key. Given (N, e) where $0 \leq \alpha \leq \frac{1}{2}$ and \widehat{d} satisfying $|d - \widehat{d}| < N^{1/4 - \epsilon}$, the private exponent can be computed in time polynomial in $\log N$ and $1/\epsilon$.*

5 Partial Key Exposure Attacks: Known LSB

In this section we consider attacks in which some of the least significant bits of the private exponent are known. In particular, we assume that the adversary knows d_0 for some (known) M such that $d \equiv d_0 \pmod{M}$. Thus, we can write the private exponent as $d = d_1M + d_0$ where d_1 is the only unknown. We will let $M = N^{\beta - \delta}$ so that the size of the unknown part of the private exponent satisfies $|d_1| < N^\delta$.

The most general partial key exposure attack on RSA with known LSB is due to Ernst et al. [14]. We extend their result to multi-prime RSA here to obtain the following new attack.

Attack 9 *For every $\epsilon > 0$ there exists an N_0 such that for every $N > N_0$ the following holds: Let N be an r -prime RSA modulus with balanced primes, let (N, e) be a valid public exponent and let (N, d) be its corresponding private key, where $e = N^\alpha$ and $d = N^\beta$. Given (N, e) , d_0 and M where $d \equiv d_0 \pmod{M}$ and $M = N^{\beta - \delta}$, if*

$$\delta \leq \frac{2}{3} + \frac{1}{3r} - \frac{2}{3r} \sqrt{(r-1)(3r\beta + 3r\alpha - 2r - 1)} - \epsilon, \quad (17)$$

then the private exponent can be recovered in time polynomial in $\log N$ and $1/\epsilon$, provided the algebraic independence assumption holds.

Proof: Beginning with the key equation, $ed = 1 + k\phi(N)$, we substitute $d = d_1M + d_0$ and $\phi(N) = N - A$ to obtain

$$eMd_1 + ed_0 = 1 + kN - kA,$$

where d_1 , k and Λ are the only unknowns. Replacing these unknowns with variables leads to the following polynomial:

$$f(x, y, z) = (eM)x - Ny + yz + ed_0 - 1 \in \mathbb{Z}[x, y, z],$$

which by construction has the integer root $(x_0, y_0, z_0) = (d_0, k, \Lambda)$. Let X , Y and Z be bounds for $|x_0|$, $|y_0|$ and $|z_0|$, respectively, defined by

$$\begin{aligned} |x_0| &= |d_0| < N^\delta = X, \\ |y_0| &= |k| = \left\lfloor \frac{ed-1}{\phi(N)} \right\rfloor < 2N^{\alpha+\beta-1} = Y, \\ |z_0| &= |\Lambda| < (2r-1)N^{1-1/r} = Z, \end{aligned}$$

and let $W = \|f(xX, yY, zX)\|_\infty$. Notice that the polynomial $f(x, y, z)$ has the same set of monomials as the polynomial in the proof of Attack 4 and that the bounds X , Y , Z and $W = \max(eMX, NY, YZ, ed_0 - 1) = NY = 2N^{\alpha+\beta}$, are also the same. From the proof of Attack 4, we can then conclude that the root (x_0, y_0, z_0) can be computed for sufficiently large N when

$$\delta \leq \frac{2}{3} + \frac{1}{3r} - \frac{2}{3r} \sqrt{(r-1)(3\alpha r + 3\beta r - 2r - 1)},$$

provided the algebraic assumption holds. \square

As with the known MSB attacks, we now consider the best partial key exposure attacks with known LSB on multi-prime RSA when only one of the private and public exponent is small. In Figure 2, we summarize these attacks for the first few values of r . As with the attacks with known MSB, we see that the effectiveness of each attack decreases with each additional prime in the modulus.

5.1 Small Private Exponent

When the private exponent is small and the keys have been chosen in the standard way then the the public exponent can be approximated, with high probability, by $e \approx N$ (i.e., $\alpha \approx 1$). Using this approximation in Attack 9, we see that, for sufficiently large N , the private exponent can be computed if

$$\delta \leq \frac{2}{3} + \frac{1}{3r} - \frac{2}{3r} \sqrt{(r-1)(3\beta r + r - 1)} - \epsilon. \quad (18)$$

Letting $r = 2$ recovers the original result $\delta \leq \frac{5}{6} - \frac{1}{3}\sqrt{1+6\beta}$, obtained by Ernst et al. [14, Theorem 3]. Combining this attack with Boneh and Durfee's small private

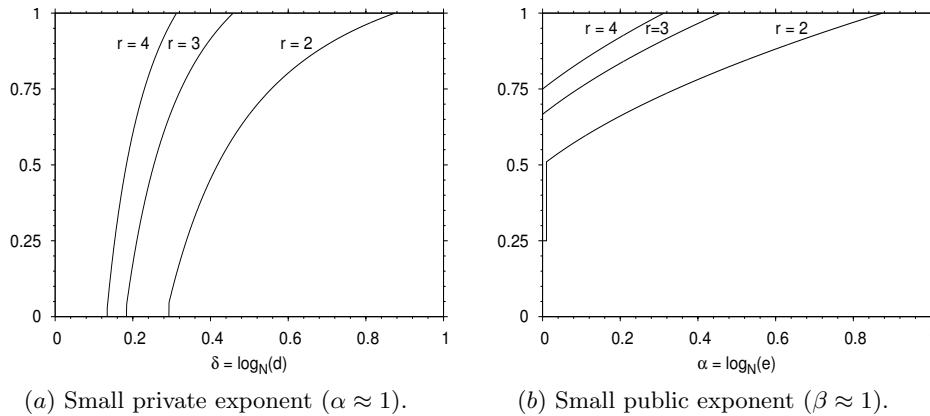


Fig. 2. Partial key exposure attacks with known LSB. In each plot, the fraction of LSB of the private exponent needed to mount the attack for large N is shown.

exponent attack gives the strongest attacks with known least significant bits. Again, we can consider Boneh and Durfee’s small private exponent attack as a partial key exposure attack in which zero of the LSB of the private exponent are needed ($\delta = 0$). We illustrate these attacks for the first few values of r in Figure 2(a).

5.2 Small Public Exponent

When the public exponent is small and the keys have been chosen in the standard way, with high probability, the private exponent can be approximated by $d \approx N$ (i.e., $\beta \approx 1$). Using this approximation in Attack 9, we see that, for sufficiently large N , the private exponent can be computed if

$$\delta \leq \frac{2}{3} + \frac{1}{3r} - \frac{2}{3r} \sqrt{(r-1)(3\alpha r + r - 1)} - \epsilon. \quad (19)$$

Letting $r = 2$ recovers the original result $\delta \leq \frac{5}{6} - \frac{1}{3}\sqrt{1+6\alpha}$, obtained by Blömer and May [2, Theorem 11], and again by Ernst et al. [14, §4.3]. In Figure 2(b), we illustrate the best known partial key exposure attacks with known LSB for instances of multi-prime RSA with small public exponent and large private exponent ($d \approx 1$) for $r \in \{2, 3, 4\}$. In addition to Attack 9, we have included Boneh, Durfee and Frankel’s small public exponent partial key exposure attack on RSA [6, Theorem 3.1], as given below.

Attack 10 *For every $\epsilon > 0$ there exists an N_0 such that for every $N > N_0$ the following holds: Let N be an r -prime RSA modulus with balanced primes, let (N, e)*

be a valid public exponent and let (N, d) be its corresponding private key, where $N \equiv 3 \pmod{4}$ and $e \leq \frac{1}{8}N^{1/4}$. Given (N, e) , d_0 and M where $d \equiv d_0 \pmod{M}$ and $M \geq N^{1/4}$, the private exponent can be computed in time polynomial in $\log N$ and $e \log e$.

When the public exponent is very small, this attack on RSA gives the strongest partial key exposure attack with known LSB. It was argued by Hinek, Low and Teske [18, §5.1], that this attack most likely cannot be extended to multi-prime RSA.

6 Partial Key Exposure Attacks: Known Partial Factorization

In this section, we extend the notion of partial key exposure attacks to include attacks in which any part of the private key, which is meant to be secret, is known. We allow the adversary to know some of the least or most significant bits of one or more of the primes in the modulus in addition to zero or more of the most or least significant bits of the private exponent. In particular, for balanced r -prime RSA we assume that the adversary knows v of the r primes in N , for some $1 \leq v \leq r - 2$, in addition to zero or more of the most or least significant bits of the remaining unknown primes and the private exponent.

We begin this section with some factoring results and then present two attacks on multi-prime RSA that recover the private exponent. The factoring attacks are simple applications of the lattice-based factoring results of Coppersmith [10] and Boneh, Durfee and Howgrave-Graham [7]. The attacks apply to any composite integer having the same form as a balanced r -prime RSA modulus. Of the attacks that recover the private exponent, the first attack recovers sufficiently small private exponents using only the public key and the partial factorization. This attack can be seen as an extension of Wiener's continued fraction attack. The second attack uses lattice basis reduction techniques based on Coppersmith's methods to improve the results of the first. This attack, like all of the other lattice-based attacks on multi-prime RSA, rely on the algebraic independence assumption and so it is only heuristic.

6.1 Factoring r -prime RSA Moduli

Boneh, Durfee and Howgrave-Graham presented a lattice-based factoring method for composite integers of the form $N = p^r q$ in [7, Theorem 3.1]. Based on their method, we present a new method to factor composite integers with the same form as multi-prime RSA moduli with balanced primes. The main result is as follows.

Attack 11 For every $\epsilon > 0$ there exists an N_0 such that for every $N > N_0$ the following holds: Let N be a balanced r -prime RSA modulus. For any $s \in [2, r]$, given $r - s$ of the primes in the factorization of N , $(s - 1)/s$ of the most or least significant bits of one of the unknown primes, $(s - 2)/(s - 1)$ of the most or least significant bits of another one of the unknown primes, \dots , $2/3$ of the most or least significant bits of another one of the unknown primes and $1/2$ of the most or least significant bits of one of the two remaining unknown primes, then N can be factored in time polynomial in r , $\log N$ and $1/\epsilon$.

Notice that Attack 11 implies an upper bound on the minimum fraction of bits needed to factor a balanced r -prime RSA modulus. In particular, sufficiently large balanced r -prime RSA moduli N can be factored given $r - s$ of the primes in N and an additional fraction of bits, relative to the size of N , given by²

$$\frac{1}{r} \times \left(\frac{s-1}{s} + \frac{s-2}{s-1} + \dots + \frac{1}{2} \right). \quad (20)$$

The actual number of bits is then roughly $\log_2 N$ times this bound. We illustrate this bound for the first few values of r and each possible choice of s in the Table 2. The table shows the fraction of bits as the sum of the contributions of the known primes and the partially known primes. The fraction is relative to the size of the modulus. In addition, we include the number of bits for a 1024-bit modulus shown in parentheses. It should be pointed out that these values (for the 1024-bit moduli) are only an estimate and are not a proven sufficient bound. The bound obtained here is in the limiting case of large moduli and is optimistic for fixed size moduli. However, the asymptotic bounds obtained in most applications of Coppersmith's methods seem to be good estimates for the actual bounds obtained in practice.

Setting $r = 2$ and $s = r$ in (20) recovers the well known result of Coppersmith [10]; that an RSA modulus can be factored with knowledge of $1/4$ of the bits of the factorization of N . In particular, $1/2$ of the most or least significant bits of one of the primes is needed. The same result can also be obtained using Boneh, Durfee and Howgrave-Graham's factoring method. In fact, the result of Attack 11 can be derived by repeatedly using Boneh, Durfee and Howgrave-Graham's factoring method to extract one partially known prime at a time until the problem is reduced to factoring a balanced RSA modulus. A proof of the attack follows.

² This sum can also be written as $\frac{1}{r} (s - \Psi(s + 1) - \gamma)$, where $\Psi(\cdot)$ is the digamma function and γ is Euler's constant.

	Number of known primes ($r - s$)			
	0	1	2	3
$r = 2$	$0 + \frac{1}{4}$ (256)			
$r = 3$	$0 + \frac{7}{18}$ (399)	$\frac{1}{3} + \frac{3}{18}$ (512)		
$r = 4$	$0 + \frac{23}{48}$ (491)	$\frac{1}{4} + \frac{14}{48}$ (555)	$\frac{2}{4} + \frac{6}{48}$ (640)	
$r = 5$	$0 + \frac{163}{300}$ (557)	$\frac{1}{5} + \frac{115}{300}$ (598)	$\frac{2}{5} + \frac{70}{300}$ (649)	$\frac{3}{5} + \frac{30}{300}$ (717)

Table 2. Fraction of bits required to factor N . Fractions are sum of the contributions of known primes and partially known primes. The values in parentheses give number of bits for a 1024-bit modulus.

Proof: [of Attack 11] First we relabel the primes so that $P = p_1 p_2 \cdots p_s$ is the product of the s unknown primes. And, without loss of generality, we assume that we know the $(s - i)/(s - i + 1)$ most or least significant bits of p_i for $i = 1, \dots, s - 1$. For each unknown prime p_i we compute \widehat{p}_i (and possibly ℓ) from the known most or least significant bits of p_i so that

$$p_i = \begin{cases} \widehat{p}_i + p_{i,0} & \text{for known MSB} \\ p_{i,0} 2^\ell + \widehat{p}_i & \text{for known LSB,} \end{cases}$$

where $p_{i,0}$ is unknown and satisfies $|p_{i,0}| < p_i^{1-(s-i)/(s-i+1)} < ((2N)^{1/r})^{1-(s-i)/(s-i+1)}$. We now compute the unknown primes one at a time; always computing the prime with the most known information first (i.e., we first compute p_1 , then p_2 , ...). In particular, for $i = 1, \dots, s - 1$, let $P_i = \left(P \times \prod_{j=1}^{i-1} p_j^{-1}\right)$ and let $f_i(x) = x + c$ where $c = \widehat{p}_i$ if the MSB of p_i are known or $c = \widehat{p}_i(2^{-\ell} \bmod P_i)$ if the LSB of p_i are known. Since P_i is the product of odd primes, the inverse of 2^ℓ is guaranteed to exist. Using Theorem 1, we compute each $p_{i,0}$ and hence p_i by finding all small roots of $f_i(x)$ modulo P_i . The result follows. \square

6.2 Small Private Exponent Attacks

Here we present two small private exponent partial key exposure attacks on multi-prime RSA. The first attack can be found in [17, Lemma 1]. The main result of the attack and a proof are given below.

Attack 12 Let N be a balanced r -prime RSA modulus, let (N, e) be a valid r -prime public key and let (N, d) be its corresponding private key where $d = N^\delta$. Given the public key and any $1 \leq v \leq r - 2$ of the primes in the factorization of N , if

$$\delta < \frac{v}{r} - \frac{v+1}{\log_2 N},$$

then d can be computed in time polynomial in $\log N$.

Proof: Let P be the product of the v known primes and $Q = N/P$. Since the primes in N are pairwise distinct we can write Euler's totient function of N as $\phi(N) = \phi(Q)\phi(P)$. This allows the key equation, $ed = 1 + k\phi(N)$, to be written as

$$ed = 1 + k\phi(Q)\phi(P), \quad (21)$$

where e and $\phi(P)$ are known quantities. Now, reducing this equation modulo $\phi(P)$ yields $d \equiv e^{-1} \pmod{\phi(P)}$ and so whenever $d < \phi(P)$ it follows that $d = e^{-1} \pmod{\phi(P)}$. Since $\phi(P) > \frac{1}{2}P > \frac{1}{2} \frac{1}{2^v} N^{v/r}$, a sufficient condition that $d < \phi(P)$ is given by $d = N^\delta < \frac{1}{2} \frac{1}{2^v} N^{v/r}$, or simply

$$\delta < \frac{v}{r} - \frac{v+1}{\log_2 N}. \quad (22)$$

Computing the inverse of e modulo $\phi(P)$ where $e, \phi(P) < N$ is polynomial in $\log_2 N$, so the result follows. \square

Since computing the inverse of e modulo $\phi(P)$ and computing the convergents of $\phi(P)/e$ are closely related, it should follow that, essentially, the same result can be obtained using the ideas in Wiener's continued fraction attack. In fact, it is straightforward to show that a sufficient condition to recover the private exponent given v of the r primes in N using the ideas of Wiener's attack is given by

$$\delta < \frac{v}{r} + \alpha - 1 - \frac{r-v+1}{\log_2 N}. \quad (23)$$

Using the approximation $\alpha \approx 1$ (since the private exponent is chosen to be small), we see that for large enough N the bounds in (22) are (23) are essentially the same. That is, if d is smaller than $N^{v/r}$ by some small multiplicative constant then d can be recovered. Using the notation in Attack 12 and its proof, we now outline a proof of this second bound. First, recall that for integers a, b, c and d , if

$$\left| \frac{a}{b} - \frac{c}{d} \right| \leq \frac{1}{2d^2},$$

then c/d is one of the convergents in the continued fraction expansion of a/b . Now, starting with the key equation $ed = 1 + k\phi(P)\phi(Q)$, we can see that

$$\left| \frac{\phi(P)}{e} - \frac{d}{k\phi(Q)} \right| = \left| \frac{1}{ek\phi(Q)} \right| \leq \frac{1}{2(k\phi(Q))^2},$$

whenever $e \geq 2k\phi(Q)$ or, equivalently, whenever $k \leq e/(2\phi(Q))$. Thus, when $k \leq e/(2\phi(Q))$, we know that $d/(k\phi(Q))$ is one of the convergents in the continued fraction expansion of $\phi(P)/e$. Since $k < d$ and $\phi(Q) \leq 2^{(r-v)}N^{(r-v)/r}$, a sufficient condition for this to hold is given by $d < 2^{-(r-v+1)}eN^{-(r-v)/r}$, or

$$\delta < \frac{v}{r} + \alpha - 1 - \frac{r-v+1}{\log_2 N}.$$

Since $\gcd(d, k) = 1$, we can simply test the numerator of each convergent until the private exponent d is found.

The second attack that we consider is new. It uses zero or more of the most significant bits of d in addition to the known factors of N to fully recover d . This attack is a generalization of Attack 4 and is an improvement of the attack found in [17, Theorem 2]. The details of the attack are as follows.

Attack 13 *For every $\epsilon > 0$ there exists an N_0 such that for every $N > N_0$ the following holds: Let N be a balanced r -prime RSA modulus, let (N, e) be a valid public exponent and let (N, d) be its corresponding private key, where $e = N^\alpha$ and $d = N^\beta$. Given (N, e) , $1 \leq v \leq r - 2$ of the primes in the factorization of N , and \widehat{d} such that $|d - \widehat{d}| \leq N^\delta$ for some $0 \leq \delta \leq \beta$, if*

$$\delta \leq \frac{2}{3} + \frac{v+1}{3r} - \frac{2}{3r} \sqrt{(r-v-1)(3r\alpha + 3r\beta - 2r - v - 1)} - \epsilon \quad (24)$$

then the private exponent can be recovered in time polynomial in $\log N$ and $1/\epsilon$, provided the algebraic independence assumption holds.

Proof: Let P be the product of the known v primes and $Q = N/P$. Starting with the key equation $ed = 1 + k\phi(P)\phi(Q)$, we can replace the private key d with $d_2 + d_1\phi(P) + d_0$ where $d_0 = e^{-1} \pmod{\phi(P)}$ and $d_2 = \widehat{d} - (\widehat{d} \pmod{\phi(P)})$. This ensures that $d \equiv d_0 \pmod{\phi(P)}$. We can also replace $\phi(Q)$ with $Q - \Lambda_Q$, where

$$\Lambda_Q < (r-v)2^{r-v-1}N^{1-\frac{v}{r}-\frac{1}{r}},$$

since the primes are balanced. Thus, we have

$$e(d_2 + d_1\phi(P) + d_0) = 1 + k\phi(P)(Q - \Lambda_Q),$$

where d_1 , k and Λ_Q are the only unknowns. Replacing each unknown with a variable leads to the following polynomial:

$$f(x, y, z) = ex - \phi(P)Qy + \phi(P)yz + d_2\phi(P) + d_0 - 1 \in \mathbb{Z}[x, y, z],$$

which by construction has the integer root $(x_0, y_0, z_0) = (d_1, k, \Lambda_Q)$. Let X , Y and Z be bounds for $|x_0|$, $|y_0|$ and $|z_0|$, respectively, defined by

$$\begin{aligned} |x_0| = |d_1| &= \left| \frac{d-d_2-d_0}{\phi(P)} \right| < 2^{v+1}N^{\delta-v/r} = X, \\ |y_0| = |k| &= \left| \frac{ed-1}{\phi(N)} \right| < 2N^{\alpha+\beta-1} = Y, \\ |z_0| = |\Lambda_Q| &< (r-v)2^{r-v-1}N^{1-\frac{v}{r}-\frac{1}{r}} = Z, \end{aligned}$$

and let $W = \|f(xX, yY, zX)\|_\infty$. Since $f(x, y, z)$ has the same set of monomials as the polynomial in Theorem 2, for any $\hat{\epsilon} > 0$ and $\tau \geq 0$ we can compute (x_0, y_0, z_0) if N is sufficiently large and

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

provided that the algebraic independence assumption holds. Substituting the values for X , Y , Z and $W = \max(e\phi(P)X, (ed_2 + ed_0 - 1), \phi(P)QY, \phi(P)YZ) = 2N^{\alpha+\beta}$, this inequality reduces to

$$(r-v-1)\tau^2 + (\delta r - 2v - 1)\tau + \frac{1}{3}(\delta r + r\beta - 2v + r\alpha - r - 1) \leq 0,$$

in the limiting case of $N \rightarrow \infty$, if we let all lower order terms and factors independent of N be absorbed into $\hat{\epsilon}$. We can minimize the left-hand side of this inequality for any choice of α , δ , r and $v \leq r - 2$ by letting $\tau = -\frac{1}{2}(\delta r - 2v - 1)/(r - v - 1)$. Using this value for τ and solving for δ , we find that

$$\delta \leq \frac{2}{3} + \frac{v+1}{3r} - \frac{2}{3r} \sqrt{(r-v-1)(3r\alpha + 3r\beta - 2r - v - 1)},$$

is a sufficient condition to recover the root (x_0, y_0, z_0) using method implicit in Theorem 2. \square

6.3 Small Private Exponent

When a small private exponent is chosen we can expect that $\alpha \approx 1$ with high probability. Using this approximation in Attack 13, we see that for sufficiently large N , the private exponent can be recovered when

$$\delta \leq \frac{2}{3} + \frac{v+1}{3r} - \frac{2}{3r} \sqrt{(r-v-1)(3\beta r + r - v - 1)} - \epsilon. \quad (25)$$

We illustrate this bound for all valid values of v for the few values of r in Figure 3. Also included in the figure is Attack 12 which gives a superior bound to Attack 13 for small enough private exponents. Notice that for fixed v (number of known primes) that the attacks are less effective with each additional prime in the modulus.

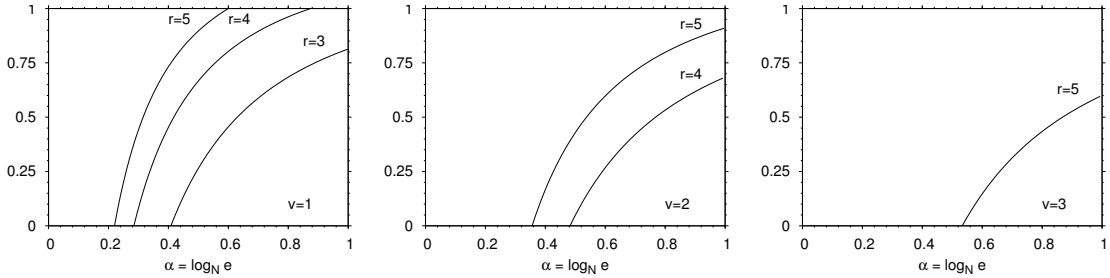


Fig. 3. Fraction of MSB, $(\beta - \delta)/\beta$, of the private exponent needed for Attack 13 with small private exponents. The plots, from left to right, are for $v = 1, 2, 3$.

6.4 Small Public Exponent

When a small public exponent is used, we can approximate the private exponent with $\beta \approx 1$ with high probability. Using this approximation in Attack 13, we see that for sufficiently large N , the private exponent can be recovered when

$$\delta \leq \frac{2}{3} + \frac{v+1}{3r} - \frac{2}{3r} \sqrt{(r-v-1)(3\alpha r + r - v - 1)} - \epsilon. \quad (26)$$

We illustrate this bound for all valid values of v for the first few values of r in In Figure 4. Notice that for fixed values of v (number of known primes) the feasible region of the attack decreases with increasing number of primes in the modulus.

Similar to Attack 5 with small public exponents, one can compute an approximation of k and try to find small solutions of a polynomial with monomials $\{x, y, z, yz\}$.

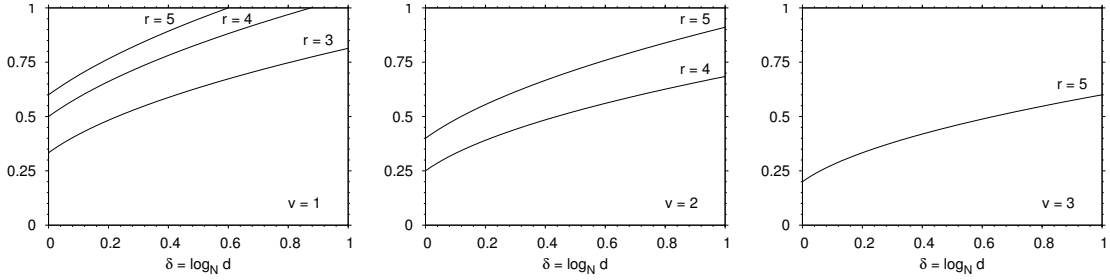


Fig. 4. Fraction of MSB, $1 - \delta$, of the private exponent needed for Attack 13 with small public exponents. The plots, from left to right, are for $v = 1, 2, 3$.

In particular, one can compute $\widehat{k} = \left\lceil \frac{e(d_2\phi(P)+d_0)-1}{\phi(P)Q} \right\rceil$, so that $k = \widehat{k} + k_0$ where $|k_0| \leq \max(\alpha + \delta - 1, \alpha + \beta - 1 - \frac{1}{r})$. It turns out that using this approximation for k does not lead to an improvement over the results of Attack 13.

It is interesting to notice that when $\beta \approx 1$ and the public exponent approaches 3 ($\alpha \approx 0$), the total number of bits required to mount the attack, including both the MSB of d and the known factors of N is $(1 - \frac{1}{r}) \log N$. This is the same number of bits of the factorization of the modulus that knowing all but one prime in the factorization would give.

7 Chinese Remainder Theorem Attack

All of the attacks in the previous sections, except for the factoring attacks in Section 2, exploit the key equation $ed = 1 + k\phi(N)$. As mentioned earlier, this equation defines the public and private exponents for textbook multi-prime RSA. In practice, however, the key generation and decryption algorithms might be different when the Chinese Remainder Theorem (CRT) is used. In particular, when decryption costs must be minimized, the key generation, encryption and decryption algorithms might be as follows:

Key Generation: Let N be the product of r randomly chosen distinct primes p_1, \dots, p_r such that $\gcd(p_1 - 1, \dots, p_r - 1) = 2$ and $\gcd(p_i - 1, p_j - 1) = 2$ for all $i \neq j$. For $i = 1, \dots, r$, choose an integer d_i satisfying $d_i < p_i - 1$ and $\gcd(d_i, p_i - 1) = 1$. Using the CRT, compute the private exponent d such that $d_i = d \bmod (p_i - 1)$ for $i = 1, \dots, r$. Compute the public exponent $e = d^{-1} \bmod (\text{lcm}(p_1 - 1, \dots, p_r - 1))$. The public key is the pair (N, e) . The private key is the $2r$ -tuple $(p_1, \dots, p_r, d_1, \dots, d_r)$.

Encryption: Same as textbook multi-prime RSA.

Decryption: For any ciphertext $c \in \mathbb{Z}_N$, the plaintext is recovered by first computing $m_i = c_i^d \bmod p_i$ for $i = 1, \dots, r$ and then combining the m_i with the CRT to recover $m = c^d \bmod N$.

The d_i values are called the CRT exponents. In order to minimize decryption costs, one simply chooses small CRT exponents. In this key generation algorithm, it is expected that both e and d will be roughly the same size as N . Therefore, none of the attacks in the previous sections, except the factoring attacks in Section 2, apply.

However, if all but one of the CRT exponents are chosen to be too small, there is one attack that factors the modulus. We give the main result below. For more details see Hinek, Low and Teske [18, §4.3].

Attack 14 *Let $N = p_1 \cdots p_r$ be an r -prime RSA modulus with balanced primes and let e be a valid public exponent with corresponding private exponent d . For $i = 1, \dots, r$, let $d_i = d \bmod (p_i - 1)$ be the CRT exponents. Let d_{SL} be the second largest CRT exponent with bitlength m . If $d_i \not\equiv d_j \pmod{2^{m/2}}$ for all $i \neq j$ then N can be factored in time $O(r\sqrt{d_{SL}} \log^2 N)$.*

Thus, the size of the CRT exponents should be chosen large enough so that the complexity of Attack 14 matches the complexity of factoring the modulus using the methods in Section 2.

Like the other factoring algorithms from Section 2, the complexity of this attack is linear in r . Essentially, the attack repeats itself $r - 1$ times obtaining one factor of N in each iteration. In practice, we have that $r \leq 5$ and most likely if $r \neq 2$ then $r = 3$. Therefore, for realistic values of r , Attack 14 is essentially independent of r .

8 Experimental Results

Here we present some experimental results to illustrate the effectiveness of the attacks from Sections 4 and 5 in practice. All computations were done with Maple [21], except for the lattice basis reduction which was done with Shoup's NTL [24]. The experiments were carried out on either a Sun Fire V100 server with one UltraSPARC IIe processor with 2GB of memory running at 550 MHz, or on a Sun Fire V440 server with four UltraSPARC IIIi processors with 8 GB of memory each running at 1.062 GHz.

For each data point obtained, we used a binary search approach to find the smallest fraction of bits needed for a successful attack for each size of the private or public

exponent considered. Each individual experiment (in the binary search) used a randomly chosen modulus with private or public exponent chosen to be a specific size. Also, unless otherwise stated, all experimental results for r -prime RSA with $r = 2, 3$ used 1024-bit moduli and all results with $r = 4$ used 2048-bit moduli. The choice of modulus size was based on Table 1 when $r = 2, 3$. While Table 1 suggests using a 4096-bit modulus when $r = 4$, we instead used a 2048-bit modulus to decrease the time for the lattice basis reduction. It is expected that

8.1 Partial Key Exposure Attacks: Known MSB

Here we show experimental results for the attacks that exploit knowledge of some of the most significant bits in the private exponent, as given in Section 4. For the first few values of r , the effectiveness of the attacks are illustrated in Figures 5 and 6 for r -prime RSA with small private exponent and small public exponent, respectively. Notice that the scale in Figure 6 has been modified.

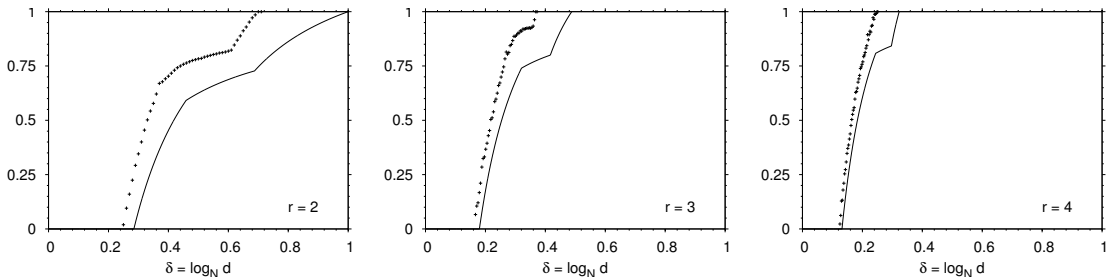


Fig. 5. Experimental fraction of MSB, $(\beta - \delta)/\beta$, of the private exponent needed to attack small private exponent multi-prime RSA with limited resources. Lower line corresponds to theoretical bound in the limit of large modulus size.

All of the attacks in Figure 5 are lattice-based. In each of the experiments the lattice used had dimension 20, which is one of the smallest lattice sizes allowed by the attacks. Already with this small lattice dimension, that attack is fairly successful compared to the theoretical bound (lower line in the plots). The lattice basis reduction took between 1–3 minutes for the experiments with $r = 2, 3$ (1024-bit moduli) and about 5–6 minutes for $r = 4$ (2048-bit moduli).

There are both latticed-based and non-lattice-based attacks illustrated in Figure 6. The non-lattice-based attacks which apply to multi-prime RSA with public exponents smaller than $N^{1/r}$ are in practice just as effective as the theory predicts.

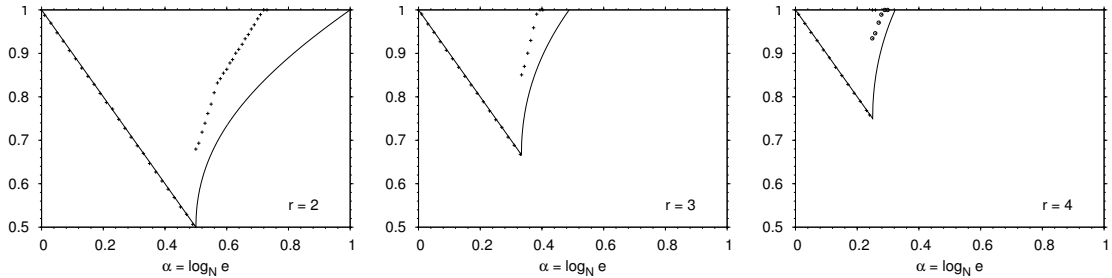


Fig. 6. Experimental fraction of MSB, $(1 - \delta)$, of the private exponent needed to attack small public exponent multi-prime RSA with limited resources. Lower line corresponds to theoretical bound in the limit of large modulus size.

In addition, these attacks are very efficient, requiring a few seconds of work with Maple. For the lattice-based attacks each experiment for $r = 2, 3$ (1024-bit moduli) used a lattice with dimension 20, with the lattice basis reduction taking roughly 1–3 minutes. Like the known MSB experiments, the attack is fairly successful compared to the theoretical bounds. When $r = 4$, however, the lattice-based attack with such a small dimension was not very successful at all. The results shown in Figure 6 for $r = 4$ are for experiments using lattices with dimension 32 with 256-bit moduli. The lattice basis reduction for these experiments required about 10 minutes. Based on other experiments, we have found that the effectiveness of the attacks are almost independent of the modulus size, so the results for $r = 4$ should be indicative of the results with same lattice dimension and 2048-bit moduli.

As mentioned in the introduction, the primary focus of this paper is the security of multi-prime RSA with more than two primes in the modulus. Thus, we only implemented attacks that apply to multi-prime RSA when the modulus has three or more primes. As a consequence, we did not investigate the practical effectiveness of the two attacks by Boneh, Durfee and Frankel that apply only to RSA (i.e., Attacks 7 and 8).

8.2 Partial Key Exposure Attacks: Known LSB

Here we show experimental results for the attacks which exploit knowledge of some of the least significant bits in the private exponent, as given in Section 5. For the first few values of r , the effectiveness of the attacks are illustrated in Figures 7 and 8 for r -prime RSA with small private exponent and small public exponent, respectively.

In Figure 7, we demonstrate the effectiveness of Attack 9 when the private exponent is small. In each of the experiments, a lattice with dimension 16 was used.

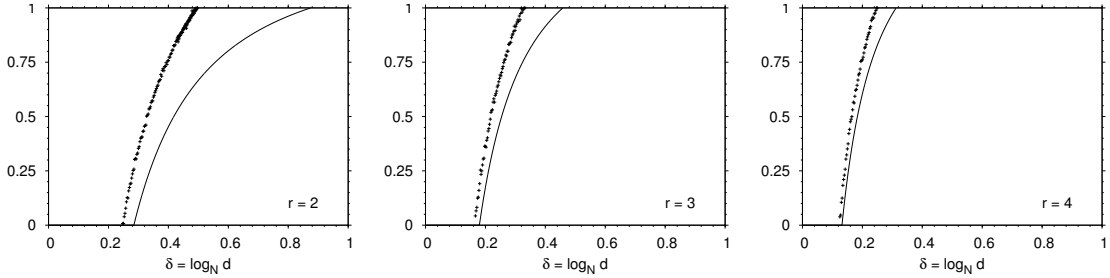


Fig. 7. Experimental fraction of LSB, $(\beta - \delta)/\beta$, of the private exponent needed to attack small private exponent multi-prime RSA with limited resources. Lower line corresponds to theoretical bound in the limit of large modulus size.

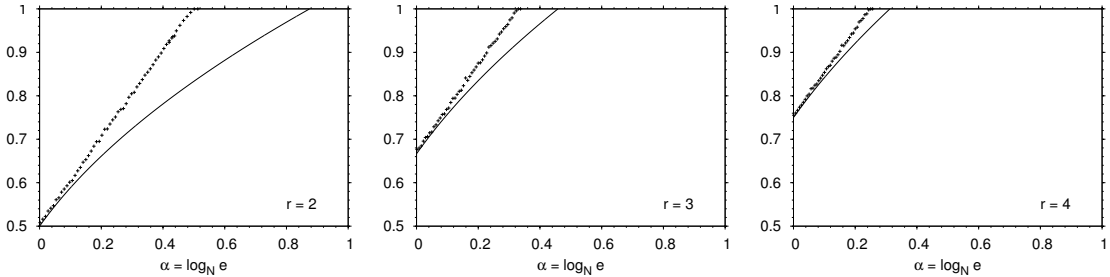


Fig. 8. Experimental fraction of LSB, $(1 - \delta)$, of the private exponent needed to attack small public exponent multi-prime RSA with limited resources. Lower line corresponds to theoretical bound in the limit of large modulus size.

The experimental bounds with such a small lattice dimension are fairly close to the theoretical bounds. The lattice basis reduction took between 1–3 minutes for the experiments with $r = 2, 3$ (1024-bit moduli) and between 5–8 minutes when $r = 4$ (2048-bit moduli). We did not investigate the effectiveness of the extension of Boneh and Durfee’s small private exponent attack, as it only applies to a very small range of private exponents not covered by the lattice-based attack in Section 5.1 and the extension of Wiener’s attack (which is much more efficient than the lattice-based attacks).

In Figure 8, we demonstrate the effectiveness of Attack 9 when the public exponent is small. In each of the experiments, a lattice with dimension 16 was used. The experimental bounds with such a small lattice dimension are fairly close to the theoretical bounds. Even when $r = 4$ (2048-bit moduli), such a small lattice yields a good experimental bound unlike the case for known MSB. The lattice basis reduction

took between 1–3 minutes for the experiments with $r = 2, 3$ (1024-bit moduli) and between 3–8 minutes when $r = 4$ (2048-bit moduli).

Again, since the primary focus of this paper is the security of multi-prime RSA with more than two primes in the modulus, we did not implement Boneh, Durfee and Frankel’s small public exponent attack on RSA (i.e., Attack 10).

8.3 Partial Key Exposure Attacks: Known Partial Factorization

We did not perform any experiments for the attacks in Section 6. The direct computation method, Attack 12, should be just as effective in practice as the theory supports since the theoretical bound is not asymptotic and does not rely on any assumptions. Also, since the lattice-based attack, Attack 13, uses the same lattice methods as the known LSB partial key exposure attacks from Section 5 the effectiveness is expected to be same as the results shown Figures 7 and 8.

9 Conclusion

We have collected, to our knowledge, the best known algebraic attacks on multi-prime RSA. Five of these attacks, Attacks 4, 5, 9, 11 and 13, are new and presented here for the first time.

There are essentially three types of attacks: The factoring attacks of Section 2; attacks on textbook multi-prime RSA; and the CRT attack. The factoring attacks from Section 2 compute the prime factorization of N given only N . For moduli with a safe number of balanced primes, the effectiveness of these attacks are essentially independent of the number of primes for a fixed modulus size. All of the attacks on textbook multi-prime RSA, Sections 3–6, exploit the key equation $ed = 1 + k\phi(N)$. In each of these attacks, the effectiveness of the attack decreases with increasing number of primes for a fixed modulus size. The CRT attack, Attack 14, requires both the public exponent e and the modulus N as input to factor the modulus (in addition to the CRT exponents being small). Like the factoring algorithms that only require knowledge of N , for realistic values of r the effectiveness of this attack is essentially independent of the number of primes for a fixed modulus size.

While the attacks collected in this work represent the current state of the art in attacks against multi-prime RSA, more research needs to be done. There are many unanswered questions about the security of multi-prime RSA. In particular, it is unknown if any partial key exposure attacks for full sized exponents exists for $r > 2$ (cf. [14] for $r = 2$), if there exist any attacks that become more effective with increasing number of primes for a fixed modulus size and if any stronger attacks on multi-prime RSA using CRT exponents exist.

References

1. 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.
2. J. Blömer and A. May. New partial key exposure attacks on RSA. In *Advances in Cryptology – Proceedings of CRYPTO 2003*, volume 2729 of *Lecture Notes in Computer Science*, pages 27–43. Springer-Verlag, 2003.
3. D. Boneh. Twenty years of attacks on the RSA cryptosystem. *Notices of the American Mathematical Society (AMS)*, 46(2):203–213, 1999.
4. D. Boneh and G. Durfee. Cryptanalysis of RSA with private key d less than $N^{0.292}$. In *Advances in Cryptology – Proceedings of EUROCRYPT '99*, volume 1592 of *Lecture Notes in Computer Science*, pages 1–11. Springer-Verlag, 1999.
5. D. Boneh, G. Durfee, and Y. Frankel. An attack on RSA given a small fraction of the private key bits. In *Advances in Cryptology – Proceedings of ASIACRYPT '98*, volume 1514 of *Lecture Notes in Computer Science*, pages 25–34. Springer-Verlag, 1998.
6. D. Boneh, G. Durfee, and Y. Frankel. Exposing an RSA private key given a small fraction of its bits. Revised and extended version of proceedings of ASIACRYPT '98 [5], 2001. Available online at <http://crypto.stanford.edu/~dabo/abstracts>.
7. D. Boneh, G. Durfee, and N. A. Howgrave-Graham. Factoring $N = p^r q$ for large r . In *Advances in Cryptology – Proceedings of CRYPTO '99*, volume 1666 of *Lecture Notes in Computer Science*, pages 326–337. Springer-Verlag, 1999.
8. 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-2002/4, Université Catholique de Louvain, 2002. Available online at http://www.dice.ucl.ac.be/crypto/tech_reports/.
9. Compaq Computer Corporation. Cryptography using Compaq multiprime technology in a parallel processing environment, 2002. Available online at <ftp://ftp.compaq.com/pub/solutions/CompaqMultiPrimeWP.pdf>.
10. D. Coppersmith. Finding a small root of a bivariate integer equation; factoring with high bits known. In *Advances in Cryptology – Proceedings of EUROCRYPT '96*, volume 1070 of *Lecture Notes in Computer Science*, pages 178–189. Springer-Verlag, 1996.
11. D. Coppersmith. Finding a small root of a univariate modular equation. In *Advances in Cryptology – Proceedings of EUROCRYPT '96*, volume 1070 of *Lecture Notes in Computer Science*, pages 155–165. Springer-Verlag, 1996.
12. D. Coppersmith. Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *Journal of Cryptology*, 10(4):233–260, 1997.
13. J.-S. Coron. Finding small roots of bivariate integer polynomial equations revisited. In *Advances in Cryptology – Proceedings of EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 492–505. Springer-Verlag, 2004.
14. M. Ernst, E. Jochemsz, A. May, and B. de Weger. Partial key exposure attacks on RSA up to full size exponents. In *Advances in Cryptology – Proceedings of EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 371–387. Springer-Verlag, 2005.
15. M. J. Hinek. Lattice attacks in cryptography: A partial overview. CACR Technical Report CACR 2004–08, Centre for Applied Cryptographic Research, University of Waterloo, 2004. Available online at <http://www.cacr.math.uwaterloo.ca/>.
16. M. J. Hinek. New partial key exposure attacks on RSA revisited. CACR Technical Report CACR 2004–02, Centre for Applied Cryptographic Research, University of Waterloo, 2004. Available online at <http://www.cacr.math.uwaterloo.ca/>.
17. M. J. Hinek. Small private exponent partial key-exposure attacks on multiprime RSA. CACR Technical Report CACR 2005–16, Centre for Applied Cryptographic Research, University of Waterloo, 2005. Available online at <http://www.cacr.math.uwaterloo.ca/>.

18. M. J. Hinek, M. K. Low, and E. Teske. On some attacks on multi-prime RSA. In *Selected Areas in Cryptography – SAC 2002*, volume 2595 of *Lecture Notes in Computer Science*, pages 385–404. Springer-Verlag, 2003.
19. N. A. 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.
20. A. K. Lenstra. Unbelievable security : Matching AES security using public key systems. In *Advances in Cryptology – Proceedings of ASIACRYPT 2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 67–86. Springer-Verlag, 2001.
21. Maplesoft. Maple 10. <http://www.maplesoft.com>.
22. A. May. Secret exponent attacks on RSA-type schemes with moduli $N = p^r q$. In *Public Key Cryptography - PKC 2004*, volume 2947 of *Lecture Notes in Computer Science*, pages 218–230. Springer-Verlag, 2004.
23. R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public key cryptosystems. *Commun. of the ACM*, 21:120–126, 1978.
24. V. Shoup. NTL: A library for doing number theory, version 5.3.2. Available online at <http://shoup.net/ntl/>.
25. H.-M. Sun and C.-T. Yang. RSA with balanced short exponents and its application to entity authentication. In *Public Key Cryptography – PKC 2005*, volume 3386 of *Lecture Notes in Computer Science*, pages 199–215. Springer-Verlag, 2005.
26. M. Wiener. Cryptanalysis of short RSA secret exponents. *IEEE Transactions on Information Theory*, 36(3):553–558, 1990.
27. P. Zimmermann. Integer factoring records. <http://www.loria.fr/~zimmerma/records/factor.html>, May 2005.