Partial Key Exposure Attack on CRT-RSA

Santanu Sarkar and Subhamoy Maitra

Indian Statistical Institute, 203 B T Road, Kolkata 700 108, India
{santanu_r,subho}@isical.ac.in

Abstract. Consider CRT-RSA with $N = pq$, $q < p < 2q$, public encryption exponent e and private decryption exponents d_p, d_q. Jochemsz and May (Crypto 2007) presented that CRT-RSA is weak when d_p, d_q are smaller than $N^{0.073}$. As a follow-up work of that paper, we study the partial key exposure attack on CRT-RSA when some Most Significant Bits (MSBs) of d_p, d_q are exposed. Further, better results are obtained when a few MSBs of p (or q) are available too. We present theoretical results as well as experimental evidences to justify our claim. We also analyze the case when the decryption exponents are of different bit sizes and it is shown that CRT-RSA is more insecure in this case (than the case of d_p, d_q having the same bit size) considering the total bit size of d_p, d_q.

Keywords: RSA, CRT-RSA, Cryptanalysis, Factorization, Lattice, LLL Algorithm, Side Channel Attacks, Weak Keys.

1 Introduction

RSA [20] is one of the most popular cryptosystems in the history of this subject. Let us first briefly describe the idea of RSA:

- primes p, q, (generally the primes are considered to be of same bit size, i.e., $q < p < 2q$);
- $N = pq$, $\phi(N) = (p-1)(q-1)$;
- e, d are such that $ed = 1 + k\phi(N)$, $k \geq 1$;
- N, e are publicly available and the plaintext $M \in \mathbb{Z}_N$ is encrypted as $C \equiv M^e \bmod N$;
- the secret key d is required to decrypt the ciphertext $C \in \mathbb{Z}_N$ as $M \equiv C^d \bmod N$.

The study of RSA is one of the most attractive areas in cryptology research as evident from many excellent works (one may refer [4,14,19] and the references therein for detailed information).

Speeding up RSA encryption and decryption is of serious interest and for large N, both e, d cannot be small at the same time. For fast encryption, it is possible to use smaller e and e as small as $2^{16} + 1$ is widely believed to be a good candidate. For fast decryption, the value of d needs to be small. However, Wiener [21] showed that when $d < \frac{1}{3}N^{\frac{1}{4}}$ then N can easily be factored. Later,

M. Abdalla et al. (Eds.): ACNS 2009, LNCS 5536, pp. 473–484, 2009.

Boneh-Durfee [5] increased this bound up to $d < N^{0.292}$. Thus the use of smaller d is in general not recommended. In this direction, an alternative approach has been proposed by Wiener [21] exploiting the Chinese Remainder Theorem (CRT) for decryption. The idea is as follows:

- the public exponent e and the private CRT exponents d_p and d_q are used satisfying $ed_p \equiv 1 \bmod (p-1)$ and $ed_q \equiv 1 \bmod (q-1)$;
- the encryption of the plaintext $M \in \mathbb{Z}_N$ is same as the standard RSA;
- to decrypt a ciphertext $C \in \mathbb{Z}_N$ one needs to compute $M_1 \equiv C^{d_p} \bmod p$ and $M_2 \equiv C^{d_q} \bmod q$;
- using CRT, one can get the plaintext M such that $M \equiv M_1 \bmod p$ and $M \equiv M_2 \bmod q$.

This variant of RSA is popularly known as CRT-RSA. Without loss of generality, consider d_p is available. One can take any random integer a in $[2, N-1]$ and then $\gcd(a^{ed_p} - a, N)$ provides p with a probability almost equal to 1 (but not exactly 1). Thus, it is clear that CRT-RSA becomes insecure if any of the decryption exponents is known. An important work in this direction shows that with the availability of decryption oracle under a fault model, one factorize N in poly$(\log N)$ time [6, Section 2.2] and the idea has been improved by A. Lenstra [6, Section 2.2, Reference 16].

May [18] described two weaknesses in CRT-RSA that work when the smaller prime factor is less than $N^{0.382}$. Bleichenbacher and May [1] improved the idea of [18] when the smaller prime factor is less than $N^{0.468}$. In [12], at attack on CRT-RSA has been presented for small e when the primes are of the same bit size. Recently, Jochemsz and May [16] presented an attack on CRT-RSA with primes of same bit size in poly$(\log N)$ time. In [16], it is shown that CRT-RSA can be attacked when the encryption exponents are of the order of N, and d_p and d_q are smaller than $N^{0.073}$. The strategy of [16] is based on the idea presented in [15] which in turn exploits the techniques from [9]. Further, in [15], it has been shown that CRT-RSA is weak if $d_p - d_q$ is known and d_p, d_q are smaller than $N^{0.099}$.

We work with techniques similar to [16], but our analysis considers that certain amounts of MSBs of d_p, d_q are exposed. This model is already accepted in literature for analysis of standard RSA, where it is considered that certain fraction of bits of the secret decryption exponent d may be exposed [3,2,11] by side channel attack. We consider a similar model in this paper. In addition, we also consider that a few MSBs of the secret prime p may be available, that can be exhaustively searched or may be known from side channel attack (as p, q are used during the decryption of CRT-RSA).

The main result of [16] was to show that for e of $O(N)$, CRT-RSA is insecure when d_p and d_q are smaller than $N^{0.073}$. Our generalization (see Theorem 2 and also Table 1 in Section 2) shows that if around $0.009 \log_2 N$ MSBs of each of d_p, d_q are exposed and $0.01 \log_2 N$ MSBs of p can be searched, then CRT-RSA is insecure when d_p and d_q are smaller than $N^{0.083}$. Our results are indeed not surprising, but the analysis we present in this paper give a clear indication how the results of [16] extend when certain amount of partial information is

available regarding the secret parameters. Our theoretical ideas are supported by experimental evidences and the results are presented in Section 2.1. The case of unbalanced decryption exponents is considered in Section 3. Section 4 concludes the paper.

1.1 Preliminaries

Let us present some basics on lattice reduction techniques. Consider the linearly independent vectors $u_1, \ldots, u_\omega \in \mathbb{Z}^n$, where $\omega \leq n$. A lattice, spanned by $\{u_1, \ldots, u_\omega\}$, is the set of all linear combinations of $u_1, \ldots, u_\omega$, i.e., ω is the dimension of the lattice. A lattice is called full rank when $\omega = n$. Let L be a lattice spanned by the linearly independent vectors $u_1, \ldots, u_\omega$, where $u_1, \ldots, u_\omega \in \mathbb{Z}^n$. By $u_1^*, \ldots, u_\omega^*$, we denote the vectors obtained by applying the Gram-Schmidt process [7, Page 81] to the vectors $u_1, \ldots, u_\omega$.

The determinant of L is defined as $\det(L) = \prod_{i=1}^{\omega} ||u_i^*||$, where $||.||$ denotes the Euclidean norm on vectors. Given a polynomial $g(x, y) = \sum a_{i,j} x^i y^j$, we define the Euclidean norm as $\| g(x, y) \| = \sqrt{\sum_{i,j} a_{i,j}^2}$ and infinity norm as $\| g(x, y) \|_\infty = \max_{i,j} |a_{i,j}|$.

It is known that given a basis $u_1, \ldots, u_\omega$ of a lattice L, the LLL algorithm [17] can find a new basis $b_1, \ldots, b_\omega$ of L with the following properties.

1. $\| b_i^* \|^2 \leq 2 \| b_{i+1}^* \|^2$, for $1 \leq i < \omega$.
2. For all i, if $b_i = b_i^* + \sum_{j=1}^{i-1} \mu_{i,j} b_j^*$ then $|\mu_{i,j}| \leq \frac{1}{2}$ for all j.
3. $\| b_i \| \leq 2^{\frac{\omega(\omega-1)+(i-1)(i-2)}{4(\omega-i+1)}} \det(L)^{\frac{1}{\omega-i+1}}$ for $i = 1, \ldots, \omega$.

By $b_1^*, \ldots, b_\omega^*$, we mean the vectors obtained by applying the Gram-Schmidt process to the vectors $b_1, \ldots, b_\omega$.

In [8], techniques have been discussed to find small integer roots of polynomials in a single variable $\bmod\ n$, and of polynomials in two variables over the integers. The idea of [8] extends to more than two variables also, but the method becomes probabilistic. The following theorem is also relevant to the idea of [8].

Theorem 1. *[13] Let $g(x, y, z, v)$ be a polynomial which is a sum of ω many monomials. Suppose $g(x_0, y_0, z_0, v_0) \equiv 0 \bmod n$, where $|x_0| < X$, $|y_0| < Y$, $|z_0| < Z$ and $|v_0| < V$. If $\| g(xX, yY, zZ, vV) \| < \frac{n}{\sqrt{\omega}}$, then $g(x_0, y_0, z_0, v_0) = 0$ holds over integers.*

Considering the property 3 mentioned above with $i = 4$ and Theorem 1, the condition $2^{\frac{\omega^2-\omega+6}{4(\omega-3)}} \det(L)^{\frac{1}{\omega-3}} < \frac{n}{\sqrt{\omega}}$ implies that if the polynomials b_1, b_2, b_3, b_4 (corresponding to the four shortest reduced basis vectors) have roots over 0 mod n, then those roots hold over integers too. The solutions corresponding to each unknown can be achieved by calculating the Gröbner basis of the ideal generated by $\{b_1, b_2, b_3, b_4\}$.

Suppose we have a set of polynomials $\{f_1, f_2, \ldots, f_i\}$ on n variables having the roots of the form $(x_{1,0}, x_{2,0}, \ldots, x_{n,0})$. Then it is known that the Gröbner

Basis [10, Page 77] $\{g_1, g_2, \ldots, g_j\}$, of $J = < f_1, f_2, \ldots, f_i >$ (the ideal generated by $\{f_1, f_2, \ldots, f_i\}$), preserves the set of common roots of $\{f_1, f_2, \ldots, f_i\}$. For our problems, we assume that the roots can be collected efficiently from $\{g_1, g_2, \ldots, g_j\}$. Though this is true in practice as noted from the experiments we perform, theoretically this may not always happen. Thus we formally state the following assumption that we will consider for the theoretical results.

Assumption 1. Consider a set of polynomials $\{f_1, f_2, \ldots, f_i\}$ on n variables having the roots of the form $(x_{1,0}, x_{2,0}, \ldots, x_{n,0})$. Let J be the ideal generated by $\{f_1, f_2, \ldots, f_i\}$. Then we will be able to collect the roots efficiently from the Gröbner Basis of J.

2 Weaknesses of CRT-RSA When Some MSBs of d_p, d_q and p Are Known

In this section, we extend the idea of [16] towards a partial key exposure attack on CRT-RSA where the secret primes are of the same bit size. We present a general result considering that some of the MSBs of d_p, d_q, p will be exposed.

Since $ed_p \equiv 1 \bmod (p-1)$ and $ed_q \equiv 1 \bmod (q-1)$, we write $ed_p = 1+k(p-1)$ and $ed_q = 1 + l(q-1)$. We start with the following technical result.

Lemma 1. *Let $e = N^\alpha$ and $d_p, d_q < N^\delta$. Consider that d_{p_0}, d_{q_0}, p_0 are exposed such that $|d_p - d_{p_0}| < N^\gamma$, $|d_q - d_{q_0}| < N^\gamma$ and $|p - p_0| < N^\beta$. Then one can find the integers k_0, l_0 such that $|k - k_0|$ and $|l - l_0|$ are $O(N^\lambda)$ where $\lambda = \max\{\alpha + \delta + \beta - 1, \alpha + \gamma - \frac{1}{2}\}$.*

Proof. We consider p, q are of same bit size, i.e., $q < p < 2q$. In such a case, $\sqrt{N} < p < \sqrt{2N}$ and $\sqrt{\frac{N}{2}} < q < \sqrt{N}$. Estimate k_0 as the closest integer value of $\frac{ed_{p_0}-1}{p_0-1}$. Also we have $k = \frac{ed_p-1}{p-1}$. Now

$$\begin{aligned}
|k - k_0| &\approx |\frac{ed_p - 1}{p-1} - \frac{ed_{p_0} - 1}{p_0 - 1}| \\
&\approx |\frac{ed_p}{p} - \frac{ed_{p_0}}{p_0}| \\
&= |\frac{ed_p p_0 - ed_p p + ed_p p - ed_{p_0} p}{pp_0}| \\
&\leq \frac{ed_p|p - p_0| + ep|d_p - d_{p_0}|}{pp_0} \\
&< \frac{N^{\alpha+\delta+\beta} + \sqrt{2}N^{\alpha+\frac{1}{2}+\gamma}}{pp_0} \text{ (as } p < \sqrt{2N}) \\
&< N^{\alpha+\delta+\beta-1} + \sqrt{2}N^{\alpha+\gamma-\frac{1}{2}} \text{ (as } pp_0 > N) \\
&< (1 + \sqrt{2})N^\lambda,
\end{aligned}$$

where $\lambda = \max\{\alpha + \delta + \beta - 1, \alpha + \gamma - \frac{1}{2}\}$. Next we calculate $q_0 = \frac{N}{p_0}$. One can check $|q - q_0| < N^\beta$. Taking l_0 as the nearest integer of $\frac{ed_{q_0}-1}{q_0-1}$, it can be shown similarly as before that $|l - l_0|$ is $O(N^\lambda)$. □

Now we will prove our main result.

Theorem 2. *Let $e = N^\alpha$ and $d_p, d_q < N^\delta$. Consider that d_{p_0}, d_{q_0}, p_0 are exposed such that $|d_p - d_{p_0}| < N^\gamma$, $|d_q - d_{q_0}| < N^\gamma$ and $|p - p_0| < N^\beta$. Let $\lambda = \max\{\alpha + \delta + \beta - 1, \alpha + \gamma - \frac{1}{2}\}$. Then, under Assumption 1, one can factor N in poly$(\log N)$ time when*

$$\gamma < \max_{\tau \geq 0} h(\tau), \text{ where } h(\tau) = \frac{(2\alpha - 3\lambda)\tau^2 + (2\alpha - \frac{10}{3}\lambda)\tau + (\frac{\alpha}{2} - \frac{5}{6}\lambda)}{2\tau^3 + \frac{5}{2}\tau^2 + \frac{4}{3}\tau + \frac{1}{3}}.$$

Proof. Suppose d_{p_0}, d_{q_0}, p_0 are exposed from d_p, d_q and p respectively. Following Lemma 1, we get the approximations k_0, l_0 of k, l respectively. Let $d_{p_1} = d_p - d_{p_0}$, $d_{q_1} = d_q - d_{q_0}$, $k_1 = k - k_0$ and $l_1 = l - l_0$. Thus, $d_{p_1}, d_{q_1}, k_1, l_1$ are unknown to the attacker.

We have $ed_p = 1 + k(p-1)$ and $ed_q = 1 + l(q-1)$. This can be re-written as $ed_p + k - 1 = kp$ and $ed_q + l - 1 = lq$. Multiplying these two equations, we get

$$e^2 d_p d_q + ed_p(l-1) + ed_q(k-1) - (N-1)kl - (k+l-1) = 0.$$

Now putting $d_p = d_{p_1} + d_{p_0}$, $d_q = d_{q_1} + d_{q_0}$, $k = k_0 + k_1$ and $l = l_0 + l_1$ in the above equation we have $e^2 d_{p_1} d_{q_1} + (e^2 d_{p_0} - e + ek_0) d_{q_1} + (e^2 d_{q_0} - e + el_0) d_{p_1} + ek_1 d_{q_1} + el_1 d_{p_1} + (ed_{q_0} - 1 - l_0 N + l_0) k_1 + (ed_{p_0} - 1 - k_0 N + k_0) l_1 + (1-N) k_1 l_1 + R = 0$, where $R = (e^2 d_{p_0} d_{q0} - ed_{p_0} - ed_{q_0} + 1 + ed_{p_0} l_0 + ed_{q_0} k_0 - l_0 k_0 N + l_0 k_0 - l_0 - k_0)$ is a known constant. Now if we substitute $d_{p_1}, d_{q_1}, k_1, l_1$ by x, y, z, v respectively then we have $e^2 xy + (e^2 d_{p_0} - e + ek_0) y + (e^2 d_{q_0} - e + el_0) x + ezy + evx + (ed_{q_0} - 1 - l_0 N + l_0) z + (ed_{p_0} - 1 - k_0 N + k_0) v + (1-N) zv + R = 0$. Hence we have to find the solution $d_{p_1}, d_{q_1}, k_1, l_1$ of the polynomial $f(x, y, z, v) = e^2 xy + (e^2 d_{p_0} - e + ek_0) y + (e^2 d_{q_0} - e + el_0) x + ezy + evx + (ed_{q_0} - 1 - l_0 N + l_0) z + (ed_{p_0} - 1 - k_0 N + k_0) v + (1-N) zv + R$. Note that this polynomial has the same monomials as of $f(x_1, x_2, x_3, x_4)$ presented in [16, Section 4], though the coefficients are different. Also, the upper bounds on the variables are different as mentioned below.

Here $d_{p_1} < N^\gamma, d_{q_1} < N^\gamma$. Also from Lemma 1, k_1, l_1 are $O(N^\lambda)$. Let $X = Y = N^\gamma$, and $Z = V = N^\lambda$, which are the upper bounds of x, y, z, v respectively (note that for the upper bounds of z, v, we have neglected the constant terms as mentioned above).

When e is significantly greater than $N^{0.5}$, then d_{p_1}, d_{q_1} are significantly smaller than k_1, l_1. As we are mostly interested for large e, we apply extra shifts on x, y as advised in the "Extended Strategy" of [15, Page 274]. In this direction we define the following as in [16]:

$$S = \bigcup_{0 \leq j \leq t} \{x^{i_1+j} y^{i_2+j} z^{i_3} w^{i_4} : x^{i_1} y^{i_2} z^{i_3} w^{i_4} \text{ is a monomial of } f^{m-1}\},$$

$$M = \{\text{monomials of } x^{i_1} y^{i_2} z^{i_3} w^{i_4} f : x^{i_1} y^{i_2} z^{i_3} w^{i_4} \in S\}.$$

That is, $x^{i_1}y^{i_2}z^{i_3}v^{i_4} \in S$ iff $i_1 = 0, \ldots, m-1-i_3+t, i_2 = 0, \ldots, m-1-i_4+t, i_3 = 0, \ldots, m-1, i_4 = 0, \ldots, m-1$, and

$x^{i_1}y^{i_2}z^{i_3}v^{i_4} \in M$ iff $i_1 = 0, \ldots, m-i_3+t, i_2 = 0, \ldots, m-i_4+t, i_3 = 0, \ldots, m, i_4 = 0, \ldots, m$ for some non-negative integer t.

We need to find at least three more polynomials f_0, f_1, f_2 that share the same root $(d_{p_1}, d_{q_1}, k_1, l_1)$ over the integers. Given $W = ||f(xX, yY, zZ, vV)||_\infty$, from [15], we know that these polynomials can be found by lattice reduction if $X^{s_1}Y^{s_2}Z^{s_3}V^{s_4} < W^s$ for $s_r = \sum_{x^{i_1}y^{i_2}z^{i_3}v^{i_4} \in M \setminus S} i_r$, $r = 1, 2, 3, 4$ and $s = |S|$.

For a given integer m and $t = \tau m$, from the definition of S and M and neglecting the lower order terms we have the required condition same as the one presented in [16, Section 4] due to the same polynomial f used in both the cases.

$$(XY)^{\frac{5}{12}+\frac{5}{3}\tau+\frac{9}{4}\tau^2+\tau^3}(ZV)^{\frac{5}{12}+\frac{5}{3}\tau+\frac{3}{2}\tau^2} < W^{\frac{1}{4}+\tau+\tau^2}. \quad (1)$$

However, the bounds on X, Y, Z, V, W are different than what presented in [16, Section 4]. As $W \geq N^{2\alpha+2\gamma}$, substituting the values of X, Y, Z, V in Inequality (1), it is enough to satisfy the following inequality:

$$(\frac{5}{12}+\frac{5}{3}\tau+\frac{9}{4}\tau^2+\tau^3)2\gamma+(\frac{5}{12}+\frac{5}{3}\tau+\frac{3}{2}\tau^2)2\lambda < (\frac{1}{4}+\tau+\tau^2)\cdot(2\alpha+2\gamma). \quad (2)$$

Thus we get the following:

$$\gamma < \frac{(2\alpha-3\lambda)\tau^2+(2\alpha-\frac{10}{3}\lambda)\tau+(\frac{\alpha}{2}-\frac{5}{6}\lambda)}{2\tau^3+\frac{5}{2}\tau^2+\frac{4}{3}\tau+\frac{1}{3}}.$$

Fixing α, λ, let $h(\tau) = \frac{(2\alpha-3\lambda)\tau^2+(2\alpha-\frac{10}{3}\lambda)\tau+(\frac{\alpha}{2}-\frac{5}{6}\lambda)}{2\tau^3+\frac{5}{2}\tau^2+\frac{4}{3}\tau+\frac{1}{3}}$. Putting $h'(\tau) = 0$, we get the equation

$$(6\lambda-4\alpha)\tau^4+(\frac{40\lambda}{3}-8\alpha)\tau^3+(\frac{28\lambda}{3}-\frac{16\alpha}{3})\tau^2+(\frac{13\lambda}{6}-\frac{7\alpha}{6})\tau = 0. \quad (3)$$

The non-negative real solutions of τ from this equation are considered and let τ_m be the value among them for which $h(\tau)$ is maximum. Putting this optimal value of τ we have $\gamma < \frac{(2\alpha-3\lambda){\tau_m}^2+(2\alpha-\frac{10}{3}\lambda)\tau_m+(\frac{\alpha}{2}-\frac{5}{6}\lambda)}{2{\tau_m}^3+\frac{5}{2}{\tau_m}^2+\frac{4}{3}\tau_m+\frac{1}{3}}$.

Under Assumption 1, we get the root using Gröbner Basis as it is done in [16] and the algorithm works in poly$(\log N)$ time. □

It can be checked that when $\beta = \frac{1}{2}$ and $\gamma = \delta$, we have the same bound as in [16].

Below we present some numerical results based on Theorem 2. We start from $\alpha = 0.4$ as the results of [16] are better than the results of [12] when $\alpha \geq 0.4$ and we follow the the technique of [16] only. Additionally we like to mention that in the proof of Theorem 2, we have assumed that e is significantly greater than $N^{0.5}$, and that actually motivates the extra shifts on the variables x, y. Thus for $e < N^{0.5}$, the results may not be optimal. While studying the numerical results, we explain two cases:

Table 1. Increased bounds of decryption exponents (that are not secure) with knowledge of some MSBs of d_p, d_q with(out) the knowledge of some MSBs of p

α	δ following		$\delta - \gamma$, when		τ_m from Theorem 2	
	[16, Section 4.1]	Theorem 2	$\beta = \frac{1}{2}$	$\beta = \frac{1}{2} - 0.01$	$\beta = \frac{1}{2}$	$\beta = \frac{1}{2} - 0.01$
0.4	0.243	0.253	0.036	0.011	0	0
0.5	0.214	0.224	0.034	0.01	0	0
0.577	0.192	0.202	0.034	0.01	0	0
0.7	0.157	0.167	0.035	0.01	0	0
0.8	0.128	0.138	0.033	0.01	0.0708	0
0.9	0.1	0.11	0.032	0.01	0.2814	0.1479
0.925	0.093	0.103	0.031	0.01	0.3411	0.1972
0.95	0.087	0.097	0.032	0.012	0.4212	0.2626
1.0	0.073	0.083	0.027	0.01	0.5563	0.3751

1. when some of the MSBs of d_p, d_q are known, but none of the bits of p is known,
2. when some of the MSBs of d_p, d_q as well as p are known.

Let us now present Table 1 based on the numerical values arising out of Theorem 2 and compare it with the values presented in [16]. We consider the asymptotic upper bound of δ presented in the table in [16, Section 7.1] (it follows the formula of [16, Section 4.1]). As we claim to improve the bound on δ with knowledge of some MSBs of d_p, d_q, we take the δ values 0.01 more than the asymptotic upper bounds presented in [16].

To get the improved bounds on δ, we need to know $(\delta - \gamma) \log_2 N$ MSBs for each of the decryption exponents. We present the values of τ_m (as in the proof of Theorem 2) given different values of α, where $h'(\tau_m) = 0$ and $h(\tau_m)$ is maximum.

The exercises are done in both the cases, (i) when none of the MSBs of p is known, i.e., $\beta = \frac{1}{2}$ and (ii) when certain amount of MSBs ($0.01 \log_2 N$ bits) of p is known.

2.1 Experimental Results

We have implemented the programs in SAGE 3.1.1 over Linux Ubuntu 8.04 on a laptop with Dual CORE Intel(R) Pentium(R) D CPU 1.83 GHz, 2 GB RAM and 2 MB Cache.

As we work with low lattice dimensions, the theoretical bounds of d_p, d_q presented in Theorem 2 may not be reached and the actual requirement of MSBs to be known will be higher in experimental results than the numerical values arrived from the theoretical results. However, we show that the values of d_p, d_q achieved in our experimental results indeed exceed the experimental evidences presented in [16]. The implementation in [16, Section 5] used Coppersmith's original method [8] instead of Coron's reformulation [9]. On the other hand, we have followed the idea of [15] based on Coron's strategy [9] itself for our experiments.

Example 1. We consider 500 bits p, q, i.e., 1000 bits $N = pq$. The primes p, q are as follows:
25798289070829351839007966808954732714009419276135431834217753205659140625211844241170852455822004088321825427467059214304525441183373237481677160066 73,
21917575359179520616765682006997748807337023829574074576681400847213872719570483692799299283517797640856385769320644474785975436506613486493416298498 09.

We consider $\alpha = 0.8$, i.e., e is an 800 bit integer as follows:
38148827244527409868150140751730507846339628911860307085692745166868047613347979370245609851753465333860864645807326653252879132195777023295307738611596524628576985135145384244469939632628502051245478337240253784616693830999966269179218595 31.

In [16, Section 7.2], it has been shown that in such a case, decryption exponents up to 79 bits are insecure in practice. The lattice parameters used in this case are $m = 2, t = 0$ and the time required to run the LLL algorithm was 2 seconds in the experimental set up of [16].

The experiment is with decryption exponents of 90 bits, where d_p, d_q are 118782450587276333036534784 3, 119758519215176582551676174 7 respectively. We consider that 36 MSBs of each of d_p, d_q and 10 MSBs of p are known. We used the lattice parameters $m = 2, t = 0$. The time required to run the LLL algorithm is 24 seconds in our experimental set up.

As referred in the proof of Theorem 2, we have f, f_0, f_1, f_2 after the LLL algorithm. Then we apply the strategy exploiting Gröbner Basis and find a polynomial on the single variable v, i.e., l_1. Once we get l_1, we find l. Consequently we can find out q since $e > N^{\frac{1}{4}}$ (one may refer to the discussion in [16, Section 7.1]). □

Example 2. We consider 500 bits p, q, i.e., 1000 bits $N = pq$. The primes p, q are as follows:
30853665252378675240326227158738086277915600253953459858065037781983730808392386668981977220226020586447166303956890040688743304881813546056 7758401737,
17488464033905098994813423905817994735525810719923764286394405145978787252987199885079995567750919151193948574185655613142299791145341725281806597704419.

We consider $\alpha = 1$, i.e., e is a 1000 bit integer as follows:
65083699058186961425207149784916366699278453927771186362888332780344776426210397065404336372536585641507633779140400587046863893781082115024775481643403861273300867952508636439489522306805166434777410416588164484028352589528592237602468293169689835348994533801849352537110236186977858341427266865574 09.

In [16, Section 7.2], it has been shown that in such a case, decryption exponents up to 15 bits are insecure in practice. The lattice parameters used in this case are $m = 3, t = 1$ and the time required to run the LLL algorithm was 13787 seconds in the experimental set up of [16].

We consider the decryption exponents of 18 bits, where d_p, d_q are 255025, 257539 respectively. We consider that 9 MSBs of each of d_p, d_q, p are known. We used the lattice parameters $m = 2, t = 1$. The time required to run the LLL algorithm is 3347 seconds in our experimental set up. □

The values of d_p, d_q in Example 2 are quite low and any one of them can be easily searched for a complete attack. Example 2 is presented only for the purpose of comparison with the result of [16].

3 Unbalanced Decryption Exponents

In this section we present similar analysis as in the earlier section, with the only difference that now the decryption exponents d_p, d_q can be of different size. Instead of considering t amount of extra shifts on both the variables x, y as in Theorem 2, here we apply two different shifts t_1, t_2 on x, y respectively. Taking two different shifts produce better results than considering the same shift in case of unbalanced decryption exponents.

Theorem 3. *Let $e = N^{\alpha}$, $d_p < N^{\delta_1}$ and $d_q < N^{\delta_2}$. Consider that d_{p_0}, d_{q_0}, p_0 are exposed such that $|d_p - d_{p_0}| < N^{\gamma_1}$, $|d_q - d_{q_0}| < N^{\gamma_2}$ and $|p - p_0| < N^{\beta}$. Let $\lambda_1 = \max\{\alpha + \delta_1 + \beta - 1, \alpha + \gamma_1 - \frac{1}{2}\}$ and $\lambda_2 = \max\{\alpha + \delta_2 + \beta - 1, \alpha + \gamma_2 - \frac{1}{2}\}$. Then, under Assumption 1, one can factor N in poly$(\log N)$ time when there exist non-negative real numbers $\tau_1, \tau_2 \geq 0$ for which $h(\tau_1, \tau_2, \gamma_1, \gamma_2, \lambda_1, \lambda_2, \alpha) = \tau_1{}^2\tau_2\gamma_1 + \tau_1\tau_2{}^2\gamma_2 + \frac{3}{4}\tau_1{}^2\gamma_1 + \frac{1}{2}\tau_1\tau_2(\gamma_1 + \gamma_2) + \frac{3}{4}\tau_2{}^2\gamma_2 + \frac{3}{2}\tau_1\tau_2(\lambda_1 + \lambda_2) - 2\tau_1\tau_2\alpha + \frac{1}{2}\tau_1\gamma_1 + \frac{1}{6}\tau_2\gamma_1 + \frac{1}{6}\tau_1\gamma_2 + \frac{1}{2}\tau_2\gamma_2 + \tau_1\lambda_1 + \frac{2}{3}\tau_2\lambda_1 + \frac{2}{3}\tau_1\lambda_2 + \tau_2\lambda_2 - \tau_1\alpha - \tau_2\alpha + \frac{1}{6}(\gamma_1 + \gamma_2) + \frac{5}{12}(\lambda_1 + \lambda_2) - \frac{\alpha}{2} < 0$.*

Proof. This proof is similar to the proof of Theorem 2 till the construction of the polynomial $f(x, y, z, v)$.

Here $d_{p_1} < N^{\gamma_1}, d_{q_1} < N^{\gamma_2}$ and we also consider $k_1 < N^{\lambda_1}, l_1 < N^{\lambda_2}$ (ignoring the constants presented in Lemma 1). Let $X = N^{\gamma_1}, Y = N^{\gamma_2}, Z = N^{\lambda_1}, V = N^{\lambda_2}$.

We have the following definitions of S, M, where t_1, t_2 are non-negative integers.

$$S = \bigcup_{0 \leq j_1 \leq t_1, 0 \leq j_2 \leq t_2} \{x^{i_1+j_1} y^{i_2+j_2} z^{i_3} w^{i_4} : x^{i_1} y^{i_2} z^{i_3} w^{i_4} \text{ is a monomial of } f^{m-1}\},$$

$$M = \{\text{monomials of } x^{i_1} y^{i_2} z^{i_3} w^{i_4} f : x^{i_1} y^{i_2} z^{i_3} w^{i_4} \in S\}.$$

Similar to the proof of Theorem 2, we need, $X^{s_1} Y^{s_2} Z^{s_3} V^{s_4} < W^s$ for $s_r = \sum_{x^{i_1} y^{i_2} z^{i_3} v^{i_4} \in M \setminus S} i_r$, $r = 1, 2, 3, 4$, $s = |S|$ and $W = ||f(xX, yY, zZ, vV)||_{\infty} \geq N^{2\alpha+\gamma_1+\gamma_2}$.

For a given integer m, let $t_1 = \tau_1 m$ and $t_2 = \tau_2 m$. Then from the definitions of S, M we have the required condition

$$X^{s_1} Y^{s_2} Z^{s_3} V^{s_4} < W^s, \tag{4}$$

where,

$s_1 = (\frac{5}{12}m^4 + m^3t_1 + \frac{3}{4}m^2{t_1}^2 + \frac{2}{3}m^3t_2 + \frac{3}{2}m^2t_1t_2 + m{t_1}^2t_2) + o(m^4)$,
$s_2 = (\frac{5}{12}m^4 + m^3t_2 + \frac{3}{4}m^2{t_2}^2 + \frac{2}{3}m^3t_1 + \frac{3}{2}m^2t_1t_2 + mt_1{t_2}^2) + o(m^4)$,
$s_3 = \frac{5}{12}m^4 + m^3t_1 + \frac{2}{3}m^3t_2 + \frac{3}{2}m^2t_1t_2 + o(m^4)$,
$s_4 = \frac{5}{12}m^4 + m^3t_2 + \frac{2}{3}m^3t_1 + \frac{3}{2}m^2t_1t_2 + o(m^4)$, and
$s = \frac{m^4}{4} + \frac{m^3(t_1+t_2)}{2} + m^2t_1t_2 + o(m^4)$.

Substituting the values of X, Y, Z, V, W in Inequality (4), and putting $t_1 = \tau_1 m$, $t_2 = \tau_2 m$, we have $(\frac{5}{12}+\tau_1+\frac{3}{4}{\tau_1}^2+\frac{2}{3}\tau_2+\frac{3}{2}\tau_1\tau_2+{\tau_1}^2\tau_2)\gamma_1+(\frac{5}{12}+\tau_2+\frac{3}{4}{\tau_2}^2+\frac{2}{3}\tau_1+\frac{3}{2}\tau_1\tau_2+\tau_1{\tau_2}^2)\gamma_2+(\frac{5}{12}+\tau_1+\frac{2}{3}\tau_2+\frac{3}{2}\tau_1\tau_2)\lambda_1+(\frac{5}{12}+\tau_2+\frac{2}{3}\tau_1+\frac{3}{2}\tau_1\tau_2)\lambda_2 < (\frac{1}{4}+\frac{\tau_1+\tau_2}{2}+\tau_1\tau_2)(2\alpha+\gamma_1+\gamma_2)$. From which we get $h(\tau_1,\tau_2,\gamma_1,\gamma_2,\lambda_1,\lambda_2,\alpha) = {\tau_1}^2\tau_2\gamma_1+\tau_1{\tau_2}^2\gamma_2+\frac{3}{4}{\tau_1}^2\gamma_1+\frac{1}{2}\tau_1\tau_2(\gamma_1+\gamma_2)+\frac{3}{4}{\tau_2}^2\gamma_2+\frac{3}{2}\tau_1\tau_2(\lambda_1+\lambda_2)-2\tau_1\tau_2\alpha+\frac{1}{2}\tau_1\gamma_1+\frac{1}{6}\tau_2\gamma_1+\frac{1}{6}\tau_1\gamma_2+\frac{1}{2}\tau_2\gamma_2+\tau_1\lambda_1+\frac{2}{3}\tau_2\lambda_1+\frac{2}{3}\tau_1\lambda_2+\tau_2\lambda_2-\tau_1\alpha-\tau_2\alpha+\frac{1}{6}(\gamma_1+\gamma_2)+\frac{5}{12}(\lambda_1+\lambda_2)-\frac{\alpha}{2} < 0$.

Then the proof follows by finding the root similar to the idea described in Theorem 2. □

One may check that putting $\tau_1 = \tau_2 = \tau$ in Theorem 3, we get the same form as presented in Theorem 2.

First consider the case, when no information about the bits of d_p, d_q, p is known. Thus, we have $\gamma_1 = \delta_1$, $\gamma_2 = \delta_2$, $\beta = \frac{1}{2}$. When δ_1, δ_2 are available, we will take the partial derivative of h with respect to τ_1, τ_2 and equate each of them to 0 to get non-negative solutions of τ_1, τ_2. Given any pair of such non-negative solutions, if h is less than zero, then for that δ_1, δ_2, CRT-RSA will be insecure.

Let us assume that for balanced d_p, d_q, CRT-RSA is insecure when $d_p, d_q < N^{\delta}$. On the other hand, consider that CRT-RSA is insecure for the unbalanced case when $d_p < N^{\delta_1}$, $d_p < N^{\delta_2}$. This situation is worth investigating when $2\delta < \delta_1 + \delta_2$. We find that this indeed happens. In [16], it has been shown that when e is $O(N)$, then CRT-RSA is insecure when $\delta = 0.073$. In Table 2, we find the cases when $\delta_1 + \delta_2$ is greater than $2\delta = 0.146$.

Table 2. Values for which CRT-RSA with unbalanced decryption exponents is insecure

δ_1	0.06	0.05	0.04	0.03
δ_2	0.087	0.099	0.111	0.126
$\delta_1 + \delta_2$	0.147	0.149	0.151	0.156

Thus considering the total amount of bits in the decryption exponents, CRT-RSA is less secure when the decryption exponents are of different bit size than the case when they are of same bit size.

In Table 3 we present the numerical results for partial key exposure attack. We consider $d_p < d_q$ and no information is available regarding the bits of d_p. Thus, we have $\gamma_1 = \delta_1$ and $(\delta_2 - \gamma_2)\log_2 N$ MSBs of d_q need to be known for the attack. Moreover, we consider two cases: (i) when no information regarding p is known and (ii) when $0.01\log_2 N$ MSBs of p are known. As a particular instance, when $d_p < N^{0.06}$, then one may attack CRT-RSA with $d_q < N^{0.097}$,

Table 3. Numerical results following Theorem 3

δ_1	δ_2	γ_2, when $\beta = \frac{1}{2}$	γ_2, when $\beta = \frac{1}{2} - 0.01$
0.03	0.136	0.102	0.122
0.04	0.121	0.091	0.107
0.05	0.109	0.078	0.093
0.06	0.097	0.068	0.082

when $(0.097 - 0.082) \log_2 N = 0.015 \log_2 N$ MSBs of d_q are exposed and also $0.01 \log_2 N$ MSBs of p is available.

For experimental results, one needs to use limited lattice dimensions and it may not be possible to reach these bounds in practice.

4 Conclusion

Using the idea of [16], we have studied the cryptanalysis of CRT-RSA when certain amount of the MSBs of the decryption exponents d_p, d_q are exposed. The attack becomes sharper with the knowledge of a few MSBs of p. The results work for any e of $O(N)$ and primes of the same bit size. Our results demonstrate that the upper bounds of insecure decryption exponents increase with the exposure of certain amounts of their MSBs. We also study the case when the decryption exponents are of different bit size. Our results show that CRT-RSA is more insecure in this case (considering the sum of bits in the decryption exponents) than when the decryption exponents are of the same bit size.

Acknowledgments. The authors like to thank the anonymous reviewers for detailed comments that improved the technical as well as editorial quality of this paper. The first author likes to acknowledge the Council of Scientific and Industrial Research (CSIR), India for supporting his research fellowship.

References

1. Bleichenbacher, D., May, A.: New Attacks on RSA with Small Secret CRT-Exponents. In: Yung, M., Dodis, Y., Kiayias, A., Malkin, T.G. (eds.) PKC 2006. LNCS, vol. 3958, pp. 1–13. Springer, Heidelberg (2006)
2. Blömer, J., May, A.: New Partial Key Exposure Attacks on RSA. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 27–43. Springer, Heidelberg (2003)
3. Boneh, D., Durfee, G., Frankel, Y.: Exposing an RSA Private Key Given a Small Fraction of its Bits. In: Ohta, K., Pei, D. (eds.) ASIACRYPT 1998. LNCS, vol. 1514, pp. 25–34. Springer, Heidelberg (1998)
4. Boneh, D.: Twenty Years of Attacks on the RSA Cryptosystem. Notices of the AMS 46(2), 203–213 (1999)
5. Boneh, D., Durfee, G.: Cryptanalysis of RSA with Private Key d Less Than $N^{0.292}$. IEEE Trans. on Information Theory 46(4), 1339–1349 (2000)
6. Boneh, D., DeMillo, R.A., Lipton, R.J.: On the importance of eliminating errors in cryptographic computations. Journal of Cryptology 14(2), 101–119 (2001)

7. Cohen, H.: A Course in Computational Algebraic Number Theory. Springer, Heidelberg (1996)
8. Coppersmith, D.: Small Solutions to Polynomial Equations and Low Exponent Vulnerabilities. Journal of Cryptology 10(4), 223–260 (1997)
9. Coron, J.-S.: Finding Small Roots of Bivariate Integer Equations Revisited. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 492–505. Springer, Heidelberg (2004)
10. Cox, D., Little, J., O'Shea, D.: Ideals, Varieties, and Algorithms, 2nd edn. Springer, Heidelberg (1998)
11. Ernst, M., Jochemsz, E., May, A., de Weger, B.: Partial Key Exposure Attacks on RSA up to Full Size Exponents. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 371–386. Springer, Heidelberg (2005)
12. Galbraith, S., Heneghan, C., Mckee, J.: Tunable Balancing of RSA. In: Boyd, C., González Nieto, J.M. (eds.) ACISP 2005. LNCS, vol. 3574, pp. 280–292. Springer, Heidelberg (2005)
13. Howgrave-Graham, N.: Finding Small Roots of Univariate Modular Equations Revisited. In: Darnell, M.J. (ed.) Cryptography and Coding 1997. LNCS, vol. 1355, pp. 131–142. Springer, Heidelberg (1997)
14. Jochemsz, E.: Cryptanalysis of RSA Variants Using Small Roots of Polynomials. Ph. D. thesis, Technische Universiteit Eindhoven (2007)
15. Jochemsz, E., May, A.: A Strategy for Finding Roots of Multivariate Polynomials with new Applications in Attacking RSA Variants. In: Lai, X., Chen, K. (eds.) ASIACRYPT 2006. LNCS, vol. 4284, pp. 267–282. Springer, Heidelberg (2006)
16. Jochemsz, E., May, A.: A Polynomial Time Attack on RSA with Private CRT-Exponents Smaller Than $N^{0.073}$. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 395–411. Springer, Heidelberg (2007)
17. Lenstra, A.K., Lenstra, H.W., Lovász, L.: Factoring Polynomials with Rational Coefficients. Mathematische Annalen 261, 513–534 (1982)
18. May, A.: Cryptanalysis of Unbalanced RSA with Small CRT-Exponent. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 242–256. Springer, Heidelberg (2002)
19. May, A.: Using LLL-Reduction for Solving RSA and Factorization Problems: A Survey. LLL+25 Conference in honour of the 25th birthday of the LLL algorithm (2007), `http://www.informatik.tu-darmstadt.de/KP/alex.html` (last accessed 23 December, 2008)
20. Rivest, R.L., Shamir, A., Adleman, L.: A Method for Obtaining Digital Signatures and Public Key Cryptosystems. Communications of ACM 21(2), 158–164 (1978)
21. Wiener, M.: Cryptanalysis of Short RSA Secret Exponents. IEEE Transactions on Information Theory 36(3), 553–558 (1990)