

Cryptanalysis of Dual CRT-RSA

Santanu Sarkar and Subhamoy Maitra

Applied Statistics Unit, Indian Statistical Institute,
203 B T Road, Kolkata 700 108, India
sarkar.santanu.bir@gmail.com, subho@isical.ac.in

Abstract. Several schemes under the framework of Dual RSA have been proposed by Sun et al (IEEE-IT, August 2007). We here concentrate on the Dual CRT-RSA scheme and present certain range of parameters for which this is insecure. As a corollary of our work, we prove that the Dual Generalized Rebalanced-RSA (Scheme III of Sun et al) can be efficiently broken for a significant region where the scheme has been claimed to be secure.

Keywords: RSA, CRT-RSA, Dual RSA, Dual CRT-RSA, Cryptanalysis, Lattices.

1 Introduction

The famous RSA public key cryptosystem has been proposed in [15] and this is possibly the most studied topic in cryptology research. An RSA modulus $N = pq$ is a product of two randomly chosen prime p, q , preferably of same bit size. The public encryption exponent e and the private decryption exponent d are such that, $ed \equiv 1 \pmod{\phi(N)}$. A plaintext $M \in \mathbb{Z}_N$ is encrypted as $C = M^e \pmod N$ and decryption is done by calculating $C^d \pmod N$.

After the invention of RSA, many of its variants are proposed and one may refer to [11, 3] as examples. In [16], another such variant of RSA, named Dual RSA, has been described. Dual RSA provides two different instances of RSA that share the same public and private exponents. Here we have two different RSA moduli $N_1 = p_1q_1, N_2 = p_2q_2$ such that the public key e and the private key d satisfies $ed \equiv 1 \pmod{\phi(N_1)}$ as well as $ed \equiv 1 \pmod{\phi(N_2)}$. In [16], the authors suggested relevant applications of Dual RSA that include blind signatures and authentication/secretcy.

To make the RSA decryption faster, the Chinese Remainder Theorem (CRT) has been exploited and the corresponding version is known as CRT-RSA [14, 17]. In this variant, there are two private exponents d_p, d_q such that $ed_p \equiv 1 \pmod{(p-1)}$ and $ed_q \equiv 1 \pmod{(q-1)}$. The encryption method is the same as it is done in RSA. To decrypt the ciphertext C , one needs to calculate $C_p \equiv C^{d_p} \pmod p$ and $C_q \equiv C^{d_q} \pmod q$. From C_p, C_q one can get the plaintext M by the application of CRT.

As CRT-RSA is faster than RSA, with the similar motivation, a CRT variant of Dual RSA has been presented in [16], which we refer as Dual CRT-RSA. This

variant consists of two different RSA moduli $N_1 = p_1q_1, N_2 = p_2q_2$ with same public exponent e and private exponents d_p, d_q . Hence in this case we have, $ed_p \equiv 1 \pmod{p_1-1} \equiv 1 \pmod{p_2-1}$ and $ed_q \equiv 1 \pmod{q_1-1} \equiv 1 \pmod{q_2-1}$. Throughout this paper we will consider N as an integer of same bit-size as of N_1, N_2 .

The key generation algorithm of Dual CRT-RSA is not known for any range of values of e, d_p, d_q . Further, for any such choice of keys, it may not be possible to obtain N_1, N_2 . An algorithm for Dual CRT-RSA key generation in a specific range has been proposed in [16, Section III C].

OUR CONTRIBUTION:

- Let $e = N^\alpha$, $\alpha > \frac{1}{4}$ and $d_p, d_q < N^\delta$. In Section 2, we show that the Dual CRT-RSA scheme is insecure when
 - $\delta < \frac{1-\alpha}{2} - \epsilon$ for a very small quantity ϵ ,
 - $\delta < \frac{3^2 4\alpha}{5}$ and $\alpha + \delta > \frac{1}{2} + \epsilon'$, for a very small quantity ϵ' .
- A method for generating certain kind of Dual CRT-RSA keys has been presented in Scheme III of [16] and it is referred as Dual Generalized Rebalanced-RSA (in short, we call it DGRR). This method can generate Dual CRT-RSA keys for $e < N^{\frac{1}{2}}$. Applying our results in Section 2, it is shown that the keys generated in DGRR are completely insecure for $N^{\frac{1}{3}} < e < N^{\frac{1}{2}}$. Further, we improve some of the existing cryptanalytic results for $e \leq N^{\frac{1}{3}}$ too. These are presented in Section 3.
- Detailed experimental results are presented in Section 4. The lattices constructed using our method are of small dimensions and hence we could perform the experiments efficiently. In fact, experimental results show that the DGRR scheme can be attacked for $e > N^{0.315}$. We also provide some justification why the experimental results sometime provide better results than our theoretical bound.

Section 5 concludes the paper.

The cryptanalytic idea exploited here are based on lattice based techniques. As in many of the results in RSA cryptanalysis (e.g., [2, 8–10]), to obtain the root of a modular polynomial we also use the seminal method of Coppersmith [4].

2 The Main Results

As $N_1 = p_1q_1$ and $N_2 = p_2q_2$, we have the following four identities for Dual CRT-RSA.

$$ed_p = 1 + k_{p_1}(p_1 - 1), \tag{1}$$

$$ed_q = 1 + k_{q_1}(q_1 - 1), \tag{2}$$

$$ed_p = 1 + k_{p_2}(p_2 - 1), \tag{3}$$

$$ed_q = 1 + k_{q_2}(q_2 - 1). \tag{4}$$

In this section we present two cryptanalytic results on Dual CRT-RSA. Let us start with the first one.

Theorem 1. Let N_1, N_2 be the public moduli of Dual CRT-RSA and $e = N^\alpha$, $d_p, d_q < N^\delta$. Consider that $g = N^\gamma$, $g_1 = N^{\gamma_1}$ and $g_2 = N^{\gamma_2}$ be such that $g = \gcd(N_1 - 1, N_2 - 1)$, $g_1 = \gcd(e, \frac{N_1 - 1}{g})$, and $g_2 = \gcd(e, \frac{N_2 - 1}{g})$. Let $\epsilon = \frac{\gamma_1 + \gamma_2 + 2\gamma}{2}$. Then, for $\alpha > \frac{1}{4}$, one can factor N_1, N_2 in $\text{poly}(\log N)$ time if $\delta < \frac{1 - \alpha}{2} - \epsilon$.

Proof. From (1), (2), we have $(ed_p - 1 + k_{p_1})(ed_q - 1 + k_{q_1}) = k_{p_1}k_{q_1}N_1$. From this we get,

$$e^2d_p d_q + e(d_p(k_{p_1} - 1) + d_q(k_{q_1} - 1)) + (1 - k_{p_1} - k_{q_1}) = (N_1 - 1)k_{p_1}k_{q_1}. \quad (5)$$

Let, $N'_1 = \frac{N_1 - 1}{gg_1}$ and $N'_2 = \frac{N_2 - 1}{gg_2}$. Now consider the polynomial

$$f_1(x_1, x_2, x_3) = e^2x_1 + ex_2 + x_3.$$

Let $y_1 = d_p d_q, y_2 = d_p(k_{p_1} - 1) + d_q(k_{q_1} - 1)$, and $y_3 = 1 - k_{p_1} - k_{q_1}$.

Clearly, $f_1(y_1, y_2, y_3) \equiv 0 \pmod{N'_1}$. Similarly, from (3), (4), we have

$$e^2d_p d_q + e(d_p(k_{p_2} - 1) + d_q(k_{q_2} - 1)) + (1 - k_{p_2} - k_{q_2}) = (N_2 - 1)k_{p_2}k_{q_2}.$$

Now assume $y_4 = d_p(k_{p_2} - 1) + d_q(k_{q_2} - 1)$ and $y_5 = 1 - k_{p_2} - k_{q_2}$. For the polynomial $f_2(x_1, x_4, x_5) = e^2x_1 + ex_4 + x_5$, we have $f_2(y_1, y_4, y_5) \equiv 0 \pmod{N'_2}$. Now using the Chinese Remainder Theorem (CRT) over the coefficients of f_1, f_2 , one can construct a polynomial

$$f_3(x_1, x_2, x_3, x_4, x_5) = a_1x_1 + a_2x_2 + a_3x_3 + a_4x_4 + a_5x_5,$$

such that $f_3(y_1, y_2, y_3, y_4, y_5) \equiv 0 \pmod{N'_1 N'_2}$.

Since $\gcd(e, N'_1) = \gcd(e, N'_2) = 1$ and $a_1 \equiv e^2 \pmod{N'_1} \equiv e^2 \pmod{N'_2}$, we have $\gcd(a_1, N'_1 N'_2) = 1$. So from f_3 , we can obtain another polynomial

$$f_4 = x_1 + b_2x_2 + b_3x_3 + b_4x_4 + b_5x_5,$$

such that $f_4(y_1, y_2, y_3, y_4, y_5) \equiv 0 \pmod{N'_1 N'_2}$. Note that $N'_1 N'_2 \approx \frac{N^2}{g^2 g_1 g_2} = N^{2 - 2\gamma - \gamma_1 - \gamma_2}$.

Let, $X_1 = N^{2\delta}, X_2 = N^{\alpha + 2\delta - \frac{1}{2}}, X_3 = N^{\alpha + \delta - \frac{1}{2}}, X_4 = N^{\alpha + 2\delta - \frac{1}{2}}, X_5 = N^{\alpha + \delta - \frac{1}{2}}$. Clearly X_1, X_2, X_3, X_4, X_5 are the upper bounds of y_1, y_2, y_3, y_4, y_5 neglecting the small constants. We want to find the modular solution of f_4 . This is a polynomial of degree 1.

Using the idea of Coppersmith [4], one can solve f_4 in $\text{poly}(\log N)$ time if

$$X_1 X_2 X_3 X_4 X_5 < N'_1 N'_2. \quad (6)$$

Putting the values of X_1, X_2, X_3, X_4 and X_5 in Inequality (6), we get

$$\delta < \frac{1 - \alpha}{2} - \frac{\gamma_1 + \gamma_2 + 2\gamma}{8}. \quad (7)$$

From the equation (5), we have $(N_1 - 1)k_{p_1}k_{q_1} \equiv 1 - k_{p_1} - k_{q_1} \pmod{e}$, i.e.,

$$\left(\frac{N_1 - 1}{gg_1}\right) gg_1 k_{p_1} k_{q_1} \equiv 1 - k_{p_1} - k_{q_1} \pmod{e}.$$

Thus when

$$gg_1k_{p_1}k_{q_1} < e, \quad (8)$$

one can calculate $gg_1k_{p_1}k_{q_1} = \left(\frac{N_1-1}{gg_1}\right)^{-1} (1-k_{p_1}-k_{q_1}) \bmod e$. Hence it is possible to obtain $k_{p_1}k_{q_1}$. Putting $g = N^\gamma, g_1 = N^{\gamma_1}, k_{p_1} \leq N^{\alpha+\delta-\frac{1}{2}}, k_{q_1} \leq N^{\alpha+\delta-\frac{1}{2}}$ in equation (8), we have

$$\delta < \frac{1-\alpha-\gamma-\gamma_1}{2}. \quad (9)$$

Since

$$\frac{1-\alpha-\gamma_1-\gamma_2-2\gamma}{2} \leq \min \left\{ \frac{1-\alpha}{2} - \frac{\gamma_1+\gamma_2+2\gamma}{8}, \frac{1-\alpha-\gamma-\gamma_1}{2} \right\},$$

the conditions (7) and (9) on δ will be satisfied if $\delta < \frac{1-\alpha-\gamma_1-\gamma_2-2\gamma}{2}$. Hence $k_{p_1} + k_{q_1}$ and $k_{p_1}k_{q_1}$ can be obtained if $\delta < \frac{1-\alpha-\gamma_1-\gamma_2-2\gamma}{2} = \frac{1-\alpha}{2} - \epsilon$, where $\epsilon = \frac{\gamma_1+\gamma_2+2\gamma}{2}$. From the knowledge of $k_{p_1} + k_{q_1}$ and $k_{p_1}k_{q_1}$, one gets k_{p_1}, k_{q_1} . Since $p_1 \equiv 1 - k_{p_1}^{-1} \bmod e$, one can factor N_1 in $\text{poly}(\log N)$ time obtaining half of the LSBs of p_1 (as explained in [2, Corollary 1]) when $\alpha > \frac{1}{4}$. The proof for factoring N_2 is similar. \square

In general g, g_1, g_2 will be small, and so $\gamma, \gamma_1, \gamma_2 \rightarrow 0$, which gives $\epsilon \rightarrow 0$. We have also found that the experimental results support this claim.

In the proof of Theorem 1, we have studied the conditions when one can collect the roots efficiently. To actually collect the roots we use Gröbner basis technique [5] and in all the experiments find polynomials of the form

$$x_3 - \frac{1-k_{p_1}-k_{q_1}}{1-k_{p_2}-k_{q_2}}y_3.$$

In all these situations, $\gcd(1-k_{p_1}-k_{q_1}, 1-k_{p_2}-k_{q_2})$ is small, that helps us to collect $1-k_{p_1}-k_{q_1}, 1-k_{p_2}-k_{q_2}$ efficiently. Directly one can not obtain y_1, y_2, y_4 , but we use the following technique to factorize N_1 and N_2 in the experiments. Moreover, in Theorem 1, we have the constraint $\alpha > \frac{1}{4}$. Using the following approach one can remove the lower bound on α .

Let $g_3 = N^{\gamma_3}$ and $g_4 = N^{\gamma_4}$ such that $g_3 = \gcd(e, N_1 - 1)$ and $g_4 = \gcd(e, N_2 - 1)$. From the knowledge of $1-k_{p_1}-k_{q_1}$ and $1-k_{p_2}-k_{q_2}$, one can find $k_{p_1}k_{q_1} \equiv a \bmod \frac{e}{g_3}$ and $k_{p_2}k_{q_2} \equiv b \bmod \frac{e}{g_4}$. So, we can write $k_{p_1}k_{q_1} = a + \frac{e}{g_3}z_1$ and $k_{p_2}k_{q_2} = b + \frac{e}{g_4}z_2$, where z_1, z_2 are unknown. Note that $z_1 \approx N^{\gamma_3+\alpha+2\delta-1}$ and $z_2 \approx N^{\gamma_4+\alpha+2\delta-1}$. Let $z_3 = k_{p_1}k_{q_1}(N_1 - 1) - k_{p_2}k_{q_2}(N_2 - 1)$. It is clear that $|z_3| \approx |k_{p_1}k_{q_1}(p_1 + q_1)| \approx N^{2\alpha+2\delta-\frac{1}{2}}$. Hence, we have to find the root (z_1, z_2, z_3) of the polynomial

$$h(x_1, x_2, x_3) = \left(a + \frac{e}{g_3}x_1\right)(N_1 - 1) - \left(b + \frac{e}{g_4}x_2\right)(N_2 - 1) - x_3.$$

Let, $X_1 = N^{\gamma_3+\alpha+2\delta-1}, X_2 = N^{\gamma_4+\alpha+2\delta-1}$ and $X_3 = N^{2\alpha+2\delta-\frac{1}{2}}$. Clearly, X_1, X_2, X_3 are the upper bounds of the z_1, z_2, z_3 . Note that

$$W = \|h(x_1X_1, x_2X_2, x_3X_3)\|_\infty \geq \frac{e}{g_3}X_1N = N^{2\alpha+2\delta}.$$

Using the idea of [4], we can find the root of h in $\text{poly}(\log N)$ time if

$$X_1 X_2 X_3 < W. \quad (10)$$

Now putting the values of X_1, X_2, X_3 and the lower bound of W in Inequality (10), we have

$$\delta < \frac{5}{8} - \frac{\alpha}{2} - \frac{\gamma_3 + \gamma_4}{4}.$$

Since $\gamma_3, \gamma_4 \rightarrow 0$ in general, the required upper bound on δ is $\delta < \frac{5}{8} - \frac{\alpha}{2}$. Note that $\frac{5}{8} - \frac{\alpha}{2} > \frac{1-\alpha}{2}$, so upper bound of δ in this case is better than the upper bound of δ in Theorem 1. After getting $k_{p_1} k_{q_1}$ and $k_{p_2} k_{q_2}$, one can factor N_1 and N_2 using the approach of [7, Section 7.5.2] when $\alpha + \delta > \frac{1}{2} + \log_N K'$ where $K' = \text{gcd}(k_{p_1} k_{q_1}, k_{p_2} k_{q_2})$.

Remark 1. The experimental results, as presented in Section 4, are better than the theoretical upper bound on δ in Theorem 1. This is because the practical runs of the LLL algorithm [12] tend to provide basis vectors that may be shorter than the estimated theoretical upper bound. Thus, it may very well happen that we may cross the upper bound of δ in Theorem 1, i.e., $\frac{1-\alpha}{2}$ (considering $\epsilon \rightarrow 0$), during the experiments. Given this, one can use the approach described above to find $k_{p_1} k_{q_1}, k_{p_2} k_{q_2}$ from the knowledge of $k_{p_1} + k_{q_1}, k_{p_2} + k_{q_2}$. This works for a higher upper bound of δ (than in Theorem 1), i.e., $\frac{5}{8} - \frac{\alpha}{2}$ (considering $\frac{\gamma_3 + \gamma_4}{4} \rightarrow 0$).

Next we present another Theorem 2 that gives better bound than that of Theorem 1 for smaller values of e .

Theorem 2. *Let N_1, N_2 be the public moduli of Dual CRT-RSA and $e = N^\alpha$, $d_p, d_q < N^\delta$. Then one can factor N_1, N_2 in $\text{poly}(\log N)$ time if $\delta < \frac{3-4\alpha}{5}$ given $\alpha + \delta > \frac{1}{2} + \epsilon'$, where $\epsilon' = \log_N(K')$, where $K' = \text{gcd}(k_{p_1} k_{q_1}, k_{p_2} k_{q_2})$.*

Proof. We have two identities:

$$e^2 d_p d_q + e(d_p(k_{p_1} - 1) + d_q(k_{q_1} - 1)) + (1 - k_{p_1} - k_{q_1}) = (N_1 - 1)k_{p_1} k_{q_1}, \quad (11)$$

$$e^2 d_p d_q + e(d_p(k_{p_2} - 1) + d_q(k_{q_2} - 1)) + (1 - k_{p_2} - k_{q_2}) = (N_2 - 1)k_{p_2} k_{q_2}. \quad (12)$$

From (11) and (12) we get,

$$e(d_q k_{p_1} + d_p k_{q_1} - d_q k_{p_2} - d_p k_{q_2}) + (-k_{p_1} - k_{q_1} + k_{p_2} + k_{q_2}) + (N_2 - 1)k_{p_2} k_{q_2} \\ = (N_1 - 1)k_{p_1} k_{q_1}. \text{ Now consider the polynomial } f = ex + y + (N_2 - 1)z.$$

Clearly,

$$f(d_q k_{p_1} + d_p k_{q_1} - d_q k_{p_2} - d_p k_{q_2}, -k_{p_1} - k_{q_1} + k_{p_2} + k_{q_2}, k_{p_2} k_{q_2}) \equiv 0 \pmod{(N_1 - 1)}.$$

Let $X = N^{\alpha+2\delta-\frac{1}{2}}, Y = N^{\alpha+\delta-\frac{1}{2}}$ and $Z = N^{2\alpha+2\delta-1}$. Then neglecting small constants, X, Y and Z will be upper bound of the modular root

$$(d_q k_{p_1} + d_p k_{q_1} - d_q k_{p_2} - d_p k_{q_2}, -k_{p_1} - k_{q_1} + k_{p_2} + k_{q_2}, k_{p_2} k_{q_2})$$

of f . From [4], one can solve f_4 in $\text{poly}(\log N)$ time if

$$XYZ < N_1 - 1. \quad (13)$$

Putting the values of X, Y, Z Inequality(13), we get

$$\delta < \frac{3 - 4\alpha}{5}. \quad (14)$$

As we have found $k_{p_2}k_{q_2}$ as the last component of the root of f , one can similarly find $k_{p_1}k_{q_1}$. After getting $k_{p_1}k_{q_1}$ and $k_{p_2}k_{q_2}$, one can factor N_1 and N_2 using the approach of [7, Section 7.5.2, Page 157] when $\alpha + \delta > \frac{1}{2} + \log_N K'$ where $K' = \text{gcd}(k_{p_1}k_{q_1}, k_{p_2}k_{q_2})$. \square

Similar to our comment on ϵ in Theorem 1, we note that in general $\epsilon' \rightarrow 0$ and this is also confirmed experimentally. Thus in the following part of this paper we always consider that $\epsilon \rightarrow 0$ as well as $\epsilon' \rightarrow 0$.

While implementing the idea of Theorem 2, we use Gröbner basis technique to collect the root and in all the experiments we obtain polynomials of the form

$$y - \frac{-k_{p_1} - k_{q_1} + k_{p_2} + k_{q_2}}{k_{p_2}k_{q_2}}z.$$

Since in all the cases $\text{gcd}(-k_{p_1} - k_{q_1} + k_{p_2} + k_{q_2}, k_{p_2}k_{q_2})$ is very small, we can successfully collect $k_{p_2}k_{q_2}$. Similarly, we can successfully collect $k_{p_1}k_{q_1}$ as well.

2.1 Comparison between Theorem 1 and Theorem 2

From the Theorems 1, 2, we get the upper bound of δ as $\frac{1-\alpha}{2}$ and $\frac{3-4\alpha}{5}$ respectively. Now, $\frac{1-\alpha}{2} < \frac{3-4\alpha}{5}$ iff $\alpha < \frac{1}{3}$. Hence, Theorem 2 will be better than Theorem 1 for $\alpha < \frac{1}{3}$. Later in Section 4, we will discuss the comparison with respect to the experimental results.

2.2 Comparison with [7]

Using continuing fraction over $\frac{N_1-1}{N_2-1}$, in [7], it is proved that when $\delta < \frac{5}{8} - \alpha$, one can find $\frac{k_{p_2}k_{q_2}}{k_{p_1}k_{q_1}}$ in the lowest terms. Using the knowledge of $\frac{k_{p_2}k_{q_2}}{k_{p_1}k_{q_1}}$, in the lowest term, one can factor N_1, N_2 in polynomial time if $\alpha + \delta > \frac{1}{2} + \log_N(K')$, where $K' = \text{gcd}(k_{p_2}k_{q_2}, k_{p_1}k_{q_1})$. Since in general K' will be of constant order, we can say one can factor N_1, N_2 using continued fraction approach if $\delta < \frac{5}{8} - \alpha$. In Theorem 1, upper bound of δ is $\frac{1-\alpha}{2}$. Thus when $\alpha > \frac{1}{4}$, our approach is better than the idea of [7]. The upper bound of δ in Theorem 2 is $\frac{3-4\alpha}{5}$. Hence, in this case, for $\alpha > \frac{1}{8}$, bound of δ in Theorem 2 is better than that of [7].

2.3 Comparison with cryptanalytic results on CRT-RSA

It is clear that the existing results on cryptanalysis of CRT-RSA will directly work on Dual CRT-RSA. Thus the region of interest is where the existing state-of-the-art cryptanalytic results on CRT-RSA cannot be used for Dual CRT-RSA.

Let us first present a brief outline of CRT-RSA cryptanalysis. May [13] identified two weaknesses in CRT-RSA that work when the smaller prime factor is less than $N^{0.382}$. Bleichenbacher and May [1] improved the result to present weaknesses when the smaller prime factor is less than $N^{0.468}$. Further, there are some results in [1] when p, q are of same bit size. In [6], an attack on CRT-RSA has been presented for small e when both the primes are of the same bit size. Jochensz and May [10] presented an attack on CRT-RSA with primes of same bit size and 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 $N^{0.073}$. Also, in [9], it has been identified that CRT-RSA is weak if $d_p - d_q$ is known and d_p, d_q are smaller than $N^{0.099}$.

Since we are considering RSA primes of same size for Dual RSA, the analysis in [1, 6, 10] are relevant here.

In [1], it is proved that when $\delta < \frac{2}{5}(1 - \alpha)$, one can factor CRT-RSA modulus efficiently. Thus as long as $\alpha < 1$, our bound of δ in Theorem 1 is better than [1]. When $\alpha < \frac{1}{2}$, our bound of δ in Theorem 2 is better than of [1]. For full bit size of e , i.e., for $\alpha = 1$ both our ideas as well as that of [1] do not work successfully towards cryptanalysis of Dual CRT-RSA.

When $\delta < \frac{1}{2} - \frac{2}{3}\alpha$, it is proved in [6] that one can factor CRT-RSA modulus efficiently. Our bound of δ in Theorem 1 is always better than of [6]. Also for $\alpha < \frac{3}{4}$, our bound of δ in Theorem 2 is better than that of [6]. For $\alpha \geq \frac{3}{4}$, both our method of Theorem 2 and idea of [6] will not work.

α	Theory of [10]		Our upper bounds on δ	
	optimal τ	upper bound of δ	Theorem 1	Theorem 2
0.10	0	0.324	0.450	0.520
0.15	0	0.314	0.425	0.480
0.20	0	0.300	0.400	0.440
0.25	0.382	0.287	0.375	0.400
0.26	0.283	0.283	0.370	0.392
0.27	0.203	0.280	0.365	0.384
0.28	0.137	0.277	0.360	0.376
0.29	0.081	0.274	0.355	0.368
0.30	0.033	0.271	0.350	0.360

Table 1. Numerical comparison of our theoretical results with that of [10].

CRT-RSA is proved to be weak in [10] in the cases when:

$$(i) \quad \delta < \frac{5-4\alpha+20\tau-16\alpha\tau+18\tau^2-12\alpha\tau^2}{14+56\tau+66\tau^2+24\tau^3},$$

$$(ii) \delta < \frac{5-4\alpha+20\tau-16\alpha\tau+27\tau^2-30\alpha\tau^2+12\tau^3-24\alpha\tau^3}{14+56\tau+66\tau^2+24\tau^3},$$

for some non-negative τ . The second bound works better than the first one for $\alpha < \frac{1}{2}$. Towards larger values of α , the first one provides better cryptanalytic bound. One can check [8, Table 5.1, Page 87] that for $\alpha \in [0.31, 0.8]$, the optimal value of τ is zero and in that case both the bounds on δ are same, which is $\frac{5-4\alpha}{14}$. For $\alpha \in [0.31, \frac{2}{3}]$, our bound in Theorem 1 is better than that of [10].

Our ideas in both Theorem 1 and Theorem 2 are better than the approach of [10] in this range as explained in Table 1. For $\alpha < 0.31$, the optimal values of τ are not zero and hence we provide numerical results as in Table 1 for [10].

2.4 Summary of our results

In Figure 1, IA, JB, KC and LD represents the lines $\delta = \frac{5}{8} - \alpha$, $\delta = \frac{3-4\alpha}{5}$, $\delta = \frac{1-\alpha}{2}$, and $\delta = \frac{5-4\alpha}{14}$ which are relevant to the upper bounds of δ in [7], Theorems 2), 1 and [10] respectively. The area $EFGHE$ shows the new region obtained from our result where Dual CRT-RSA is not secure.

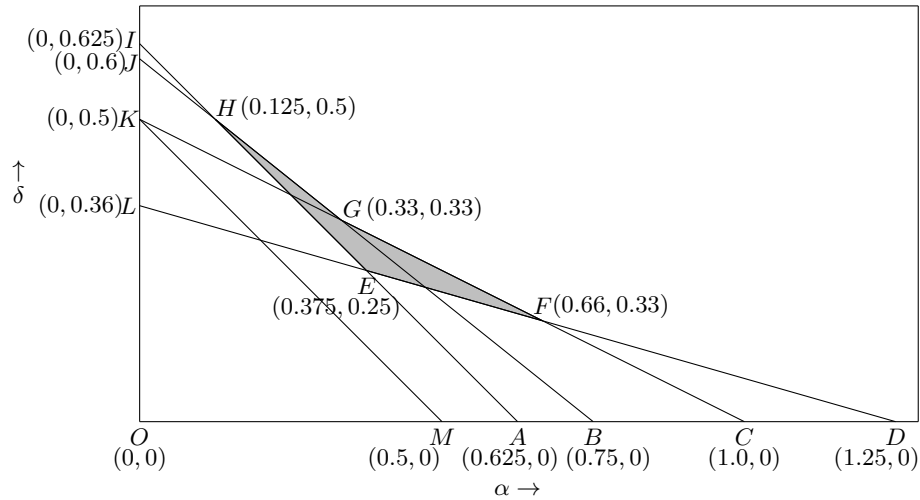


Fig. 1. New attack region is $EFGHE$.

The line KM represents $\alpha + \delta = \frac{1}{2}$. All the CRT-RSA keys (as well Dual CRT-RSA keys) must stay above this line as ed_p, ed_q are greater than $N^{\frac{1}{2}}$.

In summary, the earlier results have pointed out that the region $DEIKMD$ is insecure. In this paper, we add the region $EFGHE$ to it. Adding our result, Dual CRT-RSA is insecure in the region $DFGHKMD$.

3 Attack on DGRR

The scheme we attack here is presented in [16, Section III C]. Let n_B be the number of bits in the binary representation of an integer B . Also, in short, we write $n_N = n$. The key generation algorithm of Dual Generalized Rebalanced RSA [16] is as follows.

Input: (n_e, n_d, n_k, n) such that $n_e < n/2$ and $n_e + n_d = n/2 + n_k$.
Output: The public key (e, N_1, N_2) and the private key $(d_p, d_q, p_1, q_1, p_2, q_2)$.

- 1 Randomly select an n_e -bit integer e and set $k = \lceil \frac{n/2 - n_e}{n_k} \rceil$;
- 2 Randomly select $(k - 1)$ n_k -bit integers $p_{a_1}, \dots, p_{a_{(k-1)}}$ and an even integer p_{a_k} such that $p_a = p_{a_1} \dots p_{a_{(k-1)}} p_{a_k}$ has bit length $(n/2 - n_e)$ and $\gcd(e, p_a) = 1$;
- 3 Randomly select an n_k -bit integer k_{p_1} such that $\gcd(e, k_{p_1}) = 1$;
- 4 Compute d_p and p_b such that $ed_p = (k_{p_1} p_a) p_b + 1$, where $e < p_b < 2e$ and $k_{p_1} p_a < d_p < 2k_{p_1} p_a$. If $p_1 = p_a p_b + 1$ is not prime then go back to step 3;
- 5 If $(k_{p_1} p_a p_b / p_{a'_i}) + 1$ is prime for some $1 \leq i' \leq k - 1$ then let $p_2 = (k_{p_1} p_a p_b / p_{a'_i}) + 1$. Otherwise, go back to step 3;
- 6 Randomly select $(k - 1)$ n_k -bit integers $q_{a_1}, \dots, q_{a_{(k-1)}}$ and an even integer q_{a_k} such that $q_a = q_{a_1} \dots q_{a_{(k-1)}} q_{a_k}$ has bit length $(n/2 - n_e)$ and $\gcd(e, q_a) = 1$;
- 7 Randomly select an n_k -bit integer k_{q_1} such that $\gcd(e, k_{q_1}) = 1$;
- 8 Compute d_q and q_b such that $ed_q = (k_{q_1} q_a) q_b + 1$, where $e < q_b < 2e$ and $k_{q_1} q_a < d_q < 2k_{q_1} q_a$. If $q_1 = q_a q_b + 1$ is not prime then go back to step 7;
- 9 If $(k_{q_1} q_a q_b / q_{a'_i}) + 1$ is prime for some $1 \leq i' \leq k - 1$ then let $q_2 = (k_{q_1} q_a q_b / q_{a'_i}) + 1$. Otherwise, go back to step 7;
- 10 Calculate $N_1 = p_1 q_1$ and $N_2 = p_2 q_2$;

Algorithm 1: Key Generation Algorithm for DGRR [16].

From the key generation algorithm 1, we have the following simple result.

Lemma 1. *Let $e = N^\alpha$ and $d_p, d_q \approx N^\delta$ be the public and private exponents generated by the Algorithm 1. Then, $\delta < 1 - 2\alpha$.*

Proof. From the Step 1 in the key generation Algorithm 1, we have $n_k < \frac{n}{2} - n_e$. Also from the fact that $n_e + n_d = \frac{n}{2} + n_k$, we get $n_e + n_d < \frac{n}{2} + \frac{n}{2} - n_e$. Hence, we obtain $n_d < n - 2n_e$. As $n_e = \alpha n$ and $n_d = \delta n$, we get the desired upper bound on δ . \square

As presented in [16, Table IV], the safe parameters for DGRR is as follows:

- $n_k > \frac{n}{8} + \frac{l}{2} - 1$, where l is the exhaustive search parameter;
- $n_e + n_d > \frac{5n}{8} + \frac{l}{2} - 1$; this implies $\alpha + \delta > \frac{5}{8}$, neglecting l ;
- $5n_d + 2n_e > 2n + l$; this implies $5\delta + 2\alpha > 2$, neglecting l .

Thus the parameters proposed in [16] for which DGRR is secure is

$$\alpha < \frac{3}{8} \text{ and } \alpha + \delta > \frac{5}{8}. \quad (15)$$

Next we show that DGRR is weak for $\alpha > \frac{1}{3}$ when one uses Algorithm 1 and thus DGRR is weak even when the safe parameters are chosen as in (15).

Theorem 3. *Given the safe parameters in (15), the key generation Algorithm 1 for DGRR is insecure when*

1. (using Theorem 1) (i) $\frac{1}{3} < \alpha < \frac{3}{8}$, (ii) when $\frac{1}{4} < \alpha \leq \frac{1}{3}$ and $\delta < \frac{1-\alpha}{2}$;
2. (using Theorem 2) (i) $\frac{1}{3} < \alpha < \frac{3}{8}$, (ii) when $\frac{1}{8} < \alpha \leq \frac{1}{3}$ and $\delta < \frac{3-4\alpha}{5}$.

Proof. From Lemma 1, we know that the key generation Algorithm 1 provides DGRR keys under the constraint $\delta < 1 - 2\alpha$.

Using Theorem 1, one can factor N_1, N_2 efficiently if $\delta < \frac{1-\alpha}{2}$. Hence, when $1 - 2\alpha < \frac{1-\alpha}{2}$, i.e., when $\alpha > \frac{1}{3}$, one can break DGRR generated by the Algorithm 1. Hence given the safe parameters in (15), the key generation Algorithm 1 for DGRR is insecure when $\frac{1}{3} < \alpha < \frac{3}{8}$. Also (15) requires $\delta > \frac{5}{8} - \alpha$ and from Theorem 1, we need $\delta < \frac{1-\alpha}{2}$, which gives $\alpha > \frac{1}{4}$.

Using Theorem 2, one can factor N_1, N_2 efficiently if $\delta < \frac{3-4\alpha}{5}$. Hence, when $1 - 2\alpha < \frac{3-4\alpha}{5}$, i.e., $\alpha > \frac{1}{3}$, one can break DGRR generated by the Algorithm 1. This gives proof of item (i). Further (15) requires $\delta > \frac{5}{8} - \alpha$ and from Theorem 2, we need $\delta < \frac{3-4\alpha}{5}$. So, we need $\frac{5}{8} - \alpha < \frac{3-4\alpha}{5}$, which gives $\alpha > \frac{1}{8}$. \square

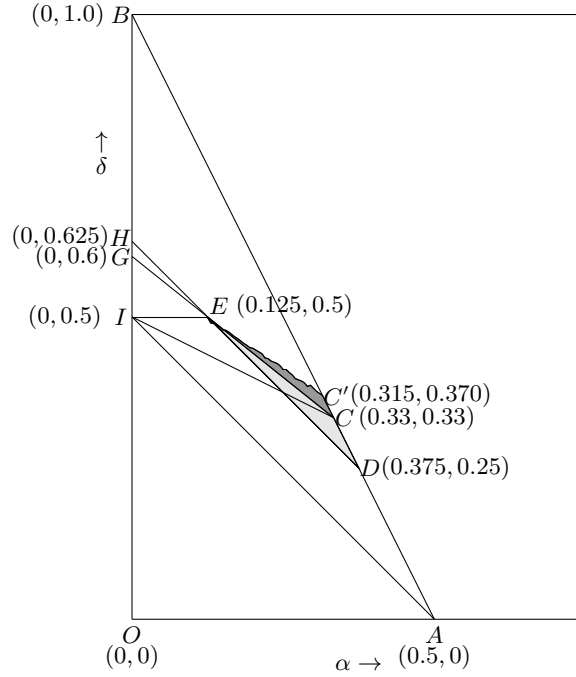


Fig. 2. Attack regions: $\triangle CDE$ (theoretical), $C'CDEC'$ (experimental).

3.1 Summary of our cryptanalysis

For DGRR, keys can be generated within $\triangle IAB$ in Figure 2. The shaded area represents the new region for which DGRR is weak. In Figure 2, IA , AB , DH , CG and CI represent the lines $\delta = \frac{1}{2} - \alpha$, $\delta = 1 - 2\alpha$, $\delta = \frac{5}{8} - \alpha$, $\delta = \frac{3-4\alpha}{5}$ and $\delta = \frac{1-\alpha}{2}$ respectively. Theoretically, $\triangle CDE$ represents our new attack region. Moreover, the experimental results show that even some regions outside $\triangle CDE$ can be vulnerable in practice and $C'DEC'$ is the extended region where DGRR is vulnerable. This is explained in more details in the following section. According to the analysis of [16], the region, where DGRR was known to be weak, has been $HDAIH$.

4 Experimental Results

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

Since our polynomial f_4 in Theorem 1 is a linear polynomial on 5 variables, the lattice dimension in our approach is only 5. Also, the polynomial f in Theorem 2 is a linear polynomial on 3 variables and hence the lattice dimension in this approach is 3.

We have implemented the idea of continuing fraction (CF) of [7]. Its experimental results are almost same as its theoretical bounds. We have also implemented the approach of [10] and in some cases its experimental results are better than the theoretical bound of itself.

In all cases we take 1000-bit N_1, N_2 . For the experiments, the Dual CRT-RSA keys are generated using Algorithm 1 [16], and we note that g, g_1, g_2 and K' are always very small. This justifies considering $\epsilon \rightarrow 0$ and $\epsilon' \rightarrow 0$.

DGRR Parameters		Upper bound δ when DGRR is not secure							
α	$1 - 2\alpha$ (upper bound of δ)	Result of [7]		Result of [10]		Theorem 1 (our)		Theorem 2 (our)	
		Theory/Expt.	Theory	Expt.	Theory	Expt.	Theory	Expt.	
0.100	0.800	0.525	0.324	0.430	0.450	0.489	0.520	0.525	
0.150	0.700	0.475	0.314	0.400	0.425	0.477	0.480	0.478	
0.200	0.600	0.425	0.300	0.370	0.400	0.445	0.440	0.436	
0.250	0.500	0.375	0.286	0.333	0.375	0.410	0.400	0.398	
0.300	0.400	0.325	0.271	0.300	0.350	0.376	0.360	0.358	
0.315	0.370	0.310	0.267	0.285	0.342	0.369	0.348	0.347	
0.350	0.300	0.275	0.257	0.260	0.325	0.299 *	0.320	0.299 *	

Table 2. Comparison our theoretical and experimental results with the existing works. Lattice Dimension in experiment of [10] is 36. In our case, it is 5 for Theorem 1 and 3 for Theorem 2. For the * marked entries, we could not generate larger d_p, d_q as we do not have any other method other than DGRR to generate the Dual CRT-RSA keys.

Let us consider the experiments corresponding to the idea of Theorem 2. When $\alpha \leq 0.1$, after lattice reduction, the coefficient of y in the first polynomial is equal to $\frac{k_{p_2}k_{q_2}}{\gcd(k_{p_1}k_{q_1}, k_{p_2}k_{q_2})}$. Since $\gcd(k_{p_1}k_{q_1}, k_{p_2}k_{q_2})$ is small, one can easily obtain $k_{p_2}k_{q_2}$. In these cases corresponding to Theorem 2, we get better experimental results than the theoretical bound.

From Lemma 1, it is clear that for $\alpha = 0.315$, the maximum possible bits of d_p, d_q is 369 ($\delta < 1 - 2\alpha = 0.370$) for 1000-bit N . From table 2, one may note that in such a situation it is possible to factor N_1, N_2 . Thus, although we have proved in Theorem 3 that DGRR is weak for $\alpha > \frac{1}{3}$, in practice DGRR becomes insecure when $\alpha > 0.315$.

5 Conclusion

In this paper we have made a disciplined study on the security of Dual CRT-RSA. We first present theoretical results to find for what kinds of keys, the Dual CRT-RSA is insecure. We note that our results identify new regions where Dual CRT-RSA can be cryptanalysed. To the best of our knowledge, these results have not been known earlier. Further, we concentrate on the Dual Generalized Rebalanced-RSA (Scheme III of [16]) and show that for a significant region in the key space, this scheme can be efficiently attacked.

References

1. D. Bleichenbacher and A. May. New attacks on RSA with small secret CRT-exponents. In Proceedings of PKC 2006, number 3958 in Lecture Notes in Computer Science, pages 1–13, Springer, 2006.
2. D. Boneh, G. Durfee and Y. Frankel. Exposing an RSA Private Key given a Small Fraction of its Bits. Asiacrypt 1998, number 1514 in Lecture Notes in Computer Science, pages 25–34, Springer, 1998.
3. D. Boneh and H. Shacham. Fast variants of RSA. *CryptoBytes*, 5(1): 1–9, 2002.
4. D. Coppersmith. Small Solutions to Polynomial Equations and Low Exponent Vulnerabilities. *Journal of Cryptology*, 10(4):223–260, 1997.
5. D. Cox, J. Little, D. O’Shea. *Ideals, Varieties, and Algorithms*. Second Edition, Springer-Verlag, 1998.
6. S. D. Galbraith, C. Heneghan, and J. F. McKee. Tunable balancing of RSA. In Proceedings of ACISP 2005, number 3574 in Lecture Notes in Computer Science, pages 280–292, Springer, 2005.
7. M. J. Hinek. On the Security of Some Variants of RSA. Ph.D. thesis, University of Waterloo, 2007. Available at <http://uwspace.uwaterloo.ca/handle/10012/2988>.
8. E. Jochemsz. Cryptanalysis of RSA Variants Using Small Roots of Polynomials. Ph.D. thesis, Technische Universiteit Eindhoven, 2007. Available at <http://www.win.tue.nl/~bdeweger/studenten.html>.
9. E. Jochemsz and A. May. A Strategy for Finding Roots of Multivariate Polynomials with new Applications in Attacking RSA Variants. In *Advances in Cryptology - Asiacrypt 2006*, number 4284 in Lecture Notes in Computer Science, pages 267–282, Springer, 2006.

10. E. Jochemsz and A. May. A polynomial time attack on RSA with private CRT-exponents smaller than $N^{0.073}$. In Advances in Cryptology - Crypto 2007, number 4622 in Lecture Notes in Computer Science, pages 395–411, Springer, 2007.
11. A. K. Lenstra and B. de Weger. Twin RSA. Mycrypt 2005, number 3715 in Lecture Notes in Computer Science, pages 222–228, Springer, 2005.
12. A. K. Lenstra, H. W. Lenstra and L. Lovász. Factoring Polynomials with Rational Coefficients. *Mathematische Annalen*, 261:513–534, 1982.
13. A. May. Cryptanalysis of Unbalanced RSA with Small CRT-Exponent. Crypto 2002, number 2442 in Lecture Notes in Computer Science, pages 242–256, Springer, 2002.
14. J. -J. Quisquater and C. Couvreur. Fast decipherment algorithm for RSA public-key cryptosystem. *Electronic Letters*, volume 18, pages 905–907, 1982.
15. R. L. Rivest, A. Shamir and L. Adleman. A Method for Obtaining Digital Signatures and Public Key Cryptosystems. *Communications of ACM*, 21(2):158–164, February 1978.
16. H. -M. Sun, M. -E. Wu, W. -C. Ting, and M. J. Hinek. Dual RSA and its applications. *IEEE Transactions on Information Theory*, 53(8):2922-2933, August 2007.
17. M. Wiener. Cryptanalysis of Short RSA Secret Exponents. *IEEE Transactions on Information Theory*, 36(3):553–558, 1990.