A new attack on RSA and CRT-RSA

No Author Given

No Institute Given

Abstract. In RSA, the public modulus $N = pq$ is the product of two primes of the same bit-size, the public exponent e and the private exponent d satisfy $ed \equiv 1 \pmod{(p-1)(q-1)}$. In many applications of RSA, d is chosen to be small. This was cryptanalyzed by Wiener in 1990 who showed that RSA is insecure if $d < N^{0.25}$. As an alternative, Quisquater and Couvreur proposed the CRT-RSA scheme in the decryption phase, where $d_p = d \pmod{(p-1)}$ and $d_q = d \pmod{(q-1)}$ are chosen significantly smaller than p and q. In 2006, Bleichenbacher and May presented an attack on CRT-RSA when the CRT-exponents d_p and d_q are both suitably small. In this paper, we show that RSA is insecure if the public exponent e satisfies an equation $ex+y \equiv 0 \pmod{p}$ with $|x||y| < N^{\frac{\sqrt{2}-1}{2}}$ and $ex+y \not\equiv 0 \pmod{N}$. As an application of our new attack, we present the cryptanalysis of CRT-RSA if one of the private exponents, d_p say, satisfies $d_p < \frac{N^{\frac{\sqrt{2}}{4}}}{\sqrt{e}}$. This improves the result of Bleichenbacher and May on CRT-RSA where both d_p and d_q are required to be suitably small.

Keywords: RSA, CRT-RSA, Cryptanalysis, Linear Modular Equation

1 Introduction

In the RSA cryptosystem, the modulus $N = pq$ is the product of two primes of the same bit-size. The public and private exponents e and d are positive integers satisfying $ed \equiv 1 \pmod{(p-1)(q-1)}$. The encryption and decryption in RSA require taking heavy exponential multiplications modulo a large integer N. To reduce the encryption time, one may be tempted to use a small public exponent e. Unfortunately, it has been proven to be insecure against some small public exponent attacks [8]. Conversely, to reduce the decryption time, one may also be tempted to use a short secret exponent d. However, it is well-known that RSA is vulnerable with a small private exponent. In 1990, Wiener [17] showed that RSA is insecure if $d < N^{0.25}$, which was extended to $d < N^{0.292}$ by Boneh and Durfee [3]. Wiener [17] proposed to use the Chinese Remainder Theorem (CRT) for decryption and Quisquater and Couvreur made this explicit in [14]. In CRT-RSA, the public exponent e and the private CRT-exponents d_p and d_q satisfy $ed_p \equiv 1 \pmod{(p-1)}$ and $ed_q \equiv 1 \pmod{(q-1)}$. One can further reduce the decryption time by carefully choosing d so that both d_p and d_q are small. Combining d_p and d_q, the CRT finds d such that $d \equiv d_p \pmod{(p-1)}$ and $d \equiv d_q \pmod{(q-1)}$. The best known attack on CRT-RSA runs in time complexity $\mathcal{O}\left(\min\left\{\sqrt{d_p}, \sqrt{d_p}\right\}\right)$ which is exponential in the bit-size of d_p or d_q. At Crypto'07, Jochemsz and May [11] proposed the first polynomial time attack on CRT exponents that are smaller than $N^{0.073}$ when p and q are balanced and e is full size, that is $\frac{e}{N} \approx 1$. In the special case when e is much smaller than N, Bleichenbacher and May [1] proposed an attack that is applicable if both d_p and d_q are such that $d_p, d_q < \min\left\{\frac{1}{4}\left(\frac{N}{e}\right)^{\frac{2}{5}}, \frac{1}{3}N^{\frac{1}{4}}\right\}$.

In this paper, we present an attack on RSA and a second attack on CRT-RSA. We consider RSA with a modulus $N = pq$ where p, q are of the same bit-size. We present an attack on RSA if one of the primes, p say, satisfies an equation $ex + y \equiv 0 \pmod{p}$, where the unknown parameters x, y satisfy

$$|x||y| < N^{\frac{\sqrt{2}-1}{2}} \text{ and } ex + y \not\equiv 0 \pmod{N}.$$

Our attack is based on the method of Coppersmith [5] for finding small solutions of modular equations. In particular, we make use of a result from Herrmann and May [9] to solve linear equations modulo divisors. Moreover, we estimate a very conservative lower bound on the number of exponents for which our method works as $N^{\frac{\sqrt{2}}{2}-\varepsilon}$ where $\varepsilon > 0$ is a small constant depending only on N. As an application of this method, we present the cryptanalysis of CRT-RSA with a private decryption exponent d_p satisfying

$$d_p < \frac{N^{\frac{\sqrt{2}}{4}}}{\sqrt{e}}.$$

We notice that for balanced p and q and small e, the attack of Bleichenbacher and May [1] works when both d_p and d_q satisfy $d_p, d_q < \min\left\{\frac{1}{4}\left(\frac{N}{e}\right)^{\frac{2}{5}}, \frac{1}{3}N^{\frac{1}{4}}\right\}$ while in our new attack, only d_p (or d_q) is required to be small.

The rest of this paper is organized as follows. In Section 2, we will state preliminaries on RSA, CRT-RSA, and bivariate linear equations modulo divisors. Section 3 will contain the description of the attack for exponents e satisfying $ex + y \equiv 0 \pmod{p}$ with suitably small parameters x, y and give a lower bound for the number of such exponents. In Section 4, we will present an application of our attack to CRT-RSA with small CRT-exponent d_p when p and q are balanced and e is much smaller than N. In Section 5, we provide some experimental results. Finally, we conclude the paper in Section 6.

2 Preliminaries

2.1 The original RSA and CRT-RSA

We first review the original RSA [15] and CRT-RSA [14].

The original RSA. The RSA cryptosystem depends on two large primes p and q used to form the RSA modulus $N = pq$. Let e and d be two integers satisfying $ed \equiv 1 \pmod{\phi(N)}$, where $\phi(N) = (p-1)(q-1)$ is the Euler totient function of N. In general, e is called the public exponent, and d is the secret exponent. To encrypt a plaintext message M, one computes the corresponding ciphertext $C \equiv M^e \pmod N$. To decrypt the ciphertext C, the receiver computes simply $M \equiv C^d \pmod N$.

CRT-RSA. In CRT-RSA, the public exponent e and the private CRT-exponents d_p and d_q satisfy $ed_p \equiv 1 \pmod{(p-1)}$ and $ed_q \equiv 1 \pmod{(q-1)}$. The CRT-RSA decryption is as follows. Compute $M_p \equiv C^{d_p} \pmod p$, $M_q \equiv C^{d_q} \pmod q$ and use the Chinese Remainder Theorem (CRT) to find M satisfying $M \equiv M_p \pmod p$ and $M \equiv M_q \pmod q$.

2.2 Bivariate linear equations modulo divisors.

In our attack we will use a theorem of Herrmann and May [9] to factor an RSA modulus $N = pq$ using a linear equation $f(x, y) = ax + by + c \equiv 0 \pmod p$. Their method is based on Coppersmith's technique for finding small roots of polynomial equations [5] and consists in using the LLL algorithm [12] to obtain two polynomials $h_1(x, y)$ and $h_2(x, y)$ sharing the same solution (x_0, y_0), that is $h_1(x_0, y_0) = h_2(x_0, y_0) = 0$. If h_1 and h_2 are algebraically independent, then the resultant of h_1 and h_2 recovers the common root (x_0, y_0). This relies on a heuristic assumption for multivariate polynomials as required by most applications of Coppersmith's algorithm [5].

Theorem 1 (Herrmann-May [9]). *Let $\varepsilon > 0$ and let N be a sufficiently large composite integer of unknown factorization with a divisor $p > N^\beta$. Furthermore, let $f(x, y) \in \mathbb{Z}[x, y]$ be a linear polynomial in two variables. Then, one can find all solutions (x_0, y_0) of the equation $f(x, y) \equiv 0 \pmod p$ with $|x_0| < N^\gamma$ and $|y_0| < N^\delta$ if*

$$\gamma + \delta \leq 3\beta - 2 + 2(1-\beta)^{\frac{3}{2}} - \varepsilon.$$

The time complexity of the algorithm is polynomial in $\log N$ and $\frac{1}{\varepsilon}$.

Let us give a sketch of the proof. First we recall two important results. The first gives a bound on the smallest vectors of an LLL-reduced lattice basis [12].

Theorem 2 (LLL [12]). *Let $\mathcal{L}$ be a lattice with dimension n and determinant $\det(\mathcal{L})$. Let $B = \langle b_1, \ldots, b_n\rangle$ be an LLL-reduced basis. Then*

$$\|b_1\| \leq \|b_2\| \leq 2^{\frac{n}{4}} (\det(\mathcal{L}))^{\frac{1}{n-1}}.$$

The next result gives a link between the roots of a polynomial modulo some integer and the roots of the polynomial over the integers. For a multivariate polynomial $f(x_1, \ldots, x_k) = \sum_{i_1,\ldots,i_k} a_{i_1,\ldots,i_k} x^{i_1} \cdots x^{i_k}$, the norm is defined as

$$\|f(x_1, \ldots, x_k)\| = \left(\sum_{i_1,\ldots,i_k} a^2_{i_1,\ldots,i_k}\right)^{\frac{1}{2}}.$$

Theorem 3 (Howgrave-Graham [10]). *Let* $f(x_1, \dots, x_k) \in \mathbb{Z}[x_1, \dots, x_k]$ *be a polynomial with at most* ω *monomials. Suppose that* $f(x_1^{(0)}, \dots, x_k^{(0)}) \equiv 0 \pmod{B}$ *where* $|x_0^{(0)}| < X_1, \dots, |x_k^{(0)}| < X_k$ *and* $\|f(X_1 x_1, \dots, X_k x_k)\| < \frac{B}{\sqrt{\omega}}$. *Then* $f(x_1^{(0)}, \dots, x_k^{(0)}) = 0$ *holds over the integers.*

We assume that $f(x, y) = x + by + c$ since otherwise we can multiply f by $a^{-1} \pmod{N}$. To find a solution (x_0, y_0) such that $f(x_0, y_0) \equiv 0 \pmod{p}$, the basic idea consists in finding two polynomials $h_1(x, y)$ and $h_2(x, y)$ such that $h_1(x_0, y_0) = h_1(x_0, y_0) = 0$ holds over the integers. Then the resultant of $h_1(x, y)$ and $h_2(x, y)$ will reveal the root (x_0, y_0). To do so, we generate a collection of polynomials $g_{k,i}(x, y)$ as

$$g_{k,i}(x, y) = y^i \cdot f(x, y)^k \cdot N^{\max\{t-k,0\}}$$

for $0 \le k \le m$, $0 \le i \le m - k$ and integer parameters t and m with $t < m$ that will be specified later. Observe that for all k and i, we have

$$g_{k,i}(x_0, y_0) = y_0^i \cdot f(x_0, y_0)^k \cdot N^{\max\{t-k,0\}} \equiv 0 \pmod{p^t}.$$

We define the following ordering for the polynomials $g_{k,i}$. If $k < l$, then $g_{k,i} < g_{l,j}$. If $k = l$ and $i < j$, then $g_{k,i} < g_{k,j}$. On the other hand, each polynomial $g_{k,i}(x, y)$ is ordered in the monomials $x^i y^k$. The ordering for the monomials $x^i y^k$ is as follows. If $i < j$, then $x^i y^k < x^j y^l$. If $i = j$ and $k < l$, then $x^i y^k < x^i y^l$. Let X and Y be positive integers. Gathering the coefficients of the polynomials $g_{k,i}(Xx, Yy)$, we obtain a matrix as illustrated in Figure 1.

	$1 \cdots y^m$	$x \cdots xy^{m-1}$	$\dots$	$x^t \cdots x^t y^{m-t}$	$\cdots$	x^m
$g_{0,0}$	N^t					
$\vdots$	$\ddots$					
$g_{0,m}$	$N^t Y^m$					
$g_{1,0}$	$* \dots *$	$N^{t-1} X$				
$\vdots$	$* \cdots *$	$\ddots$				
$g_{1,m-1}$	$* \cdots *$	$* \dots N^{t-1} X Y^{m-1}$				
$\vdots$	$* \vdots *$	$* \vdots *$	$\ddots$			
$g_{t,0}$	$* \dots *$	$* \dots *$	$\dots$	X^t		
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$		
$g_{t,m-t}$	$* \cdots *$	$* \dots *$	$\dots$	$* \dots X^t Y^{m-t}$		
$\vdots$	$* \vdots *$	$* \vdots *$	$\vdots$	$* \vdots *$	$\ddots$	
$g_{m,0}$	$* \cdots *$	$* \dots *$	$\dots$	$* \dots *$	$\dots$	X^m

Fig. 1. Herrmann-May's matrix of the polynomials $g_{k,i}(Xx, Yy)$ in the basis $\langle x^r y^s \rangle_{0 \le r \le m, 0 \le s \le m-r}$.

Let $\mathcal{L}$ be the lattice of row vectors from the coefficients of the polynomials $g_{k,i}(Xx, Yy)$ in the basis $\langle x^k y^i \rangle_{0\leq k\leq m, 0\leq i\leq m-k}$. The dimension of $\mathcal{L}$ is

$$n = \sum_{i=0}^{m}(m+1-i) = \frac{(m+2)(m+1)}{2}.$$

From the triangular matrix of the lattice, we can easily compute the determinant $\det(\mathcal{L}) = X^{s_x} Y^{s_y} N^{s_N}$ where

$$s_x = \sum_{i=0}^{m} i(m+1-i) = \frac{m(m+1)(m+2)}{6},$$
$$s_y = \sum_{i=0}^{m}\sum_{j=0}^{m-i} j = \frac{m(m+1)(m+2)}{6},$$
$$s_N = \sum_{i=0}^{t}(t-i)(m+1-i) = \frac{t(t+1)(3m+4-t)}{6}.$$

We want to find two polynomials with short coefficients that contain all small roots over the integer. This can be achieved by applying the LLL algorithm [12] to the lattice $\mathcal{L}$. From Theorem 2, we get two polynomials $h_1(x, y)$ and $h_2(x, y)$ satisfying

$$\|h_1(Xx, Yy)\| \leq \|h_2(Xx, Yy)\| \leq 2^{\frac{n}{4}} (\det(\mathcal{L}))^{\frac{1}{n-1}}.$$

To ensure that (x_0, y_0) is a root of both $h_1(x, y)$ and $h_2(x, y)$ over the integers, we apply Howgrave-Graham's Theorem 3 for $h_1(Xx, Yy)$ and $h_2(Xx, Yy)$ with $B = p^t$ and $\omega = n$. A sufficient condition is that

$$2^{n/4}(\det(\mathcal{L}))^{1/(n-1)} \leq \frac{p^t}{\sqrt{n}}. \tag{1}$$

Let $X = N^\gamma$, $Y = N^\delta$ and $p > N^\beta$ with $\beta \geq \frac{1}{2}$. We have $n = \frac{(m+2)(m+1)}{2}$ and $\det(\mathcal{L}) = X^{s_x} Y^{s_y} N^{s_N} = N^{s_x(\gamma+\delta)+s_N}$. Then the condition (1) transforms to

$$2^{\frac{(m+2)(m+1)}{8}} N^{\frac{2(\gamma+\delta)s_x+2s_N}{m(m+3)}} \leq \frac{N^{\beta t}}{\sqrt{\frac{(m+2)(m+1)}{2}}}. \tag{2}$$

Define $\varepsilon_1 > 0$ such that

$$\frac{2^{-\frac{(m+2)(m+1)}{8}}}{\sqrt{\frac{(m+2)(m+1)}{2}}} = N^{-\varepsilon_1}.$$

Then, the condition (2) simplifies to

$$\frac{2(\gamma+\delta)s_x + 2s_N}{m(m+3)} \leq \beta t - \varepsilon_1.$$

Neglecting the ε_1 term and using $s_x = \frac{m(m+1)(m+2)}{6}$ and $s_N = \frac{t(t+1)(3m+4-t)}{6}$, we get

$$\frac{m(m+1)(m+2)}{3}(\gamma+\delta) + \frac{t(t+1)(3m+4-t)}{3} < m(m+3)\beta t.$$

It is shown in [9] that setting $t = \left(1-\sqrt{1-\beta}\right)m$, this leads to the condition

$$\gamma+\delta < 3\beta - 2 + 2(1-\beta)^{\frac{3}{2}} - \varepsilon,$$

with a small constant $\varepsilon > 0$ and that the method's complexity is polynomial in $\log(N)$ and $1/\varepsilon$.

3 A New Class of Weak Public Exponents in RSA

In this section, we analyze the security of the RSA cryptosystem where the public exponent e satisfies an equation $ex+y \equiv 0 \pmod p$ with parameters x and y satisfying $ex+y \not\equiv 0 \pmod N$ $|x| < N^\gamma$ and $|y| < N^\delta$ with $\gamma+\delta \leq \frac{\sqrt{2}-1}{2}$. We firstly show that such exponents lead to the factorization of the RSA modulus and secondly that a very conservative estimate for the number of such weak exponents is $N^{\frac{1}{2}-\varepsilon}$ where $\varepsilon > 0$ is arbitrarily small for suitably large N.

Theorem 4. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let e be a public exponent satisfying an equation $ex+y \equiv 0 \pmod p$ with $|x| < N^\gamma$ and $|y| < N^\delta$. If $ex+y \not\equiv 0 \pmod N$ and*

$$\gamma+\delta \leq \frac{\sqrt{2}-1}{2},$$

then N can be factored in polynomial time.

Proof. Let $N = pq$ be an RSA modulus with $q < p < 2q$. Then $N < p^2$ and $\sqrt{N} < p$. Hence $p = N^\beta$ for some $\beta > \frac{1}{2}$. Let e be a public exponent satisfying an equation $ex+y \equiv 0 \pmod p$, which is linear in the two variables x and y. Assume that $|x| < N^\gamma$ and $|y| < N^\delta$ with γ and δ satisfying

$$\gamma+\delta \leq \frac{\sqrt{2}-1}{2}.$$

Then applying Theorem 1 with any $\beta > \frac{1}{2}$, we find x and y in polynomial time. Using x and y, we get $ex+y = pz$ for some integer z. Moreover, assume that $ex+y \not\equiv 0 \pmod N$. Then $\gcd(z,q) = 1$. Hence

$$\gcd(ex+y, N) = \gcd(pz, N) = p.$$

This terminates the proof. □

Next, we estimate the number of exponents for which our method works.

Theorem 5. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. The number of exponents $e < N$ satisfying $ex + y \equiv 0 \pmod p$ and $ex + y \not\equiv 0 \pmod N$ where $\gcd(x, y) = 1$, $|x| < N^\gamma$ and $|y| < N^\delta$, with*

$$\gamma + \delta \le \frac{\sqrt{2}-1}{2},$$

is at least $N^{\frac{\sqrt{2}}{2}-\varepsilon}$ where ε is a small positive constant.

Proof. Consider the set

$$\begin{aligned}\mathcal{K} = \{e \ :\ & 2 \le e < N,\ e = \alpha p + \left(-yx^{-1} \pmod p\right), \text{with } \gcd(x, y) = 1, \\ & 0 \le \alpha < q,\ |x| < N^\gamma,\ |y| < N^{\frac{\sqrt{2}-1}{2}-\gamma} \text{ and } ex + y \not\equiv 0 \pmod N\}.\end{aligned}$$

Here $\left(-yx^{-1} \pmod p\right)$ represents the unique positive integer lying in the interval $(0, p-1)$. Each exponent $e \in \mathcal{K}$ satisfies $ex + y \equiv 0 \pmod p$ where x and y fulfil the condition of Theorem 4. Moreover, $ex + y \not\equiv 0 \pmod N$. Hence, we can apply Theorem 4 to find the parameters x and y related to each exponent $e \in \mathcal{K}$. This shows that every exponent $e \in \mathcal{K}$ is vulnerable to the attack.

Next, let $e_1 \in \mathcal{K}$ and $e_2 \in \mathcal{K}$ with

$$e_1 = \alpha_1 p + \left(-y_1 x_1^{-1} \pmod p\right), \quad e_2 = \alpha_2 p + \left(-y_2 x_2^{-1} \pmod p\right).$$

Suppose $e_1 = e_2$. Then $e_1 \equiv e_2 \pmod p$ and $-y_1 x_1^{-1} \equiv -y_2 x_2^{-1} \pmod p$. Equivalently, we get $y_1 x_1^{-1} - y_2 x_2^{-1} \equiv 0 \pmod p$. Multiplying by $x_1 x_2$ modulo p, we get $y_1 x_2 - y_2 x_1 \equiv 0 \pmod p$. On the other hand, for $i = 1, 2$, we have $x_i, y_i \le N^{\frac{\sqrt{2}-1}{2}}$. Hence, since $q < p < 2q$ and $\sqrt{N} < p$, we get

$$|y_1 x_2 - y_2 x_1| \le |y_1 x_2| + |y_2 x_1| \le 2N^{2\times\frac{\sqrt{2}-1}{2}} = 2N^{\sqrt{2}-1} < N^{\frac{1}{2}} < p.$$

This implies that $y_1 x_2 - y_2 x_1 = 0$ and since $(x_1, y_1) = 1$ and $(x_2, y_2) = 1$, then $x_1 = x_2$ and $y_1 = y_2$. Hence $e_1 = e_2$ reduces to $\alpha_1 p = \alpha_2 p$ and $\alpha_1 = \alpha_2$. This shows that each exponent $e \in \mathcal{K}$ is defined by a unique tuple (α, x, y). Observe that if e satisfies $ex + y \equiv 0 \pmod p$ and $ex + y \equiv 0 \pmod q$ with $x < q$, then $ex + y \equiv 0 \pmod N$ and $e \equiv -yx^{-1} \pmod N$. To find an estimation of $\#\mathcal{K}$, consider the set

$$\begin{aligned}\mathcal{K}' = \{e \ :\ & 2 \le e < N,\ e = \left(-yx^{-1} \pmod N\right), \\ & \text{with } \gcd(x, y) = 1\ , |x| < N^\gamma,\ |y| < N^{\frac{\sqrt{2}-1}{2}-\gamma}\}.\end{aligned}$$

On the other hand, observe that the conditions $|x| < N^\gamma$ and $|y| < N^{\frac{\sqrt{2}-1}{2}-\gamma}$ imply that $|x||y| < N^{\frac{\sqrt{2}-1}{2}}$. Let

$$M = \left\lfloor N^{\frac{\sqrt{2}-1}{2}} \right\rfloor.$$

The number $\#\mathcal{K}$ of exponents $e \in \mathcal{K}$ is such that

$$\begin{aligned}
\#\mathcal{K} &\geq \sum_{\alpha=0}^{q-1} \sum_{|x|=1}^{M} \sum_{\substack{|y|=1 \\ (x,y)=1}}^{M/|x|} 1 - \#\mathcal{K}' \\
&\geq q \sum_{|x|=1}^{M} \sum_{\substack{|y|=1 \\ (x,y)=1}}^{M/|x|} 1 - \sum_{|x|=1}^{M} \sum_{\substack{|y|=1 \\ (x,y)=1}}^{M/|x|} 1 \\
&\geq (q-1) \sum_{|x|=1}^{M} \sum_{\substack{|y|=1 \\ (x,y)=1}}^{M/|x|} 1 \\
&\geq (q-1)M.
\end{aligned}$$

Since $q - 1 = N^{\frac{1}{2}-\varepsilon_1}$ and $M = N^{\frac{\sqrt{2}-1}{2}-\varepsilon_2}$ for some $\varepsilon_1 > 0$ and $\varepsilon_2 > 0$, then

$$\#\mathcal{K} > N^{\frac{1}{2}-\varepsilon_1} \times N^{\frac{\sqrt{2}-1}{2}-\varepsilon_2} = N^{\frac{\sqrt{2}}{2}-\varepsilon},$$

where $\varepsilon > 0$ is a small constant. This terminates the proof. $\square$

4 Application to CRT-RSA

In this section, we present a new attack on CRT-RSA. Let $N = pq$ be an RSA modulus. Let e be a public exponent corresponding to the private exponent d. Since the attacks of Wiener [17] and Boneh and Durfee [3], we know that RSA with a small private key d is vulnerable. As an alternative approach, Wiener proposed to use the Chinese Remainder Theorem (CRT) for decryption. Then Quisquater and Couvreur proposed a decryption scheme in [14]. The scheme uses two private exponents d_p and d_q related to d by

$$d_p \equiv d \pmod{(p-1)}, \qquad d_q \equiv d \pmod{(q-1)}.$$

Many attacks on CRT-RSA show that using small d_p and d_q is also dangerous. The best known result from Jochemsz and May [11] asserts that CRT-RSA is vulnerable if d_p and d_q are smaller than $N^{0.073}$.

Notice that the private exponents d_p and d_q satisfy the equations

$$ed_p \equiv 1 \pmod{(p-1)}, \qquad ed_q \equiv 1 \pmod{(q-1)}.$$

Rewriting the equation $ed_p \equiv 1 \pmod{(p-1)}$ as $ed_p = 1 + k_p(p-1)$ where k_p is a positive integer, we get $ed_p = 1 - k_p + k_p p$, and $ed_p + k_p - 1 \equiv 0 \pmod{p}$. It follows that $(d_p, k_p - 1)$ is a solution of the equation $ex + y \equiv 0 \pmod{p}$ in the variables (x, y). Hence one can apply Theorem 4 which leads to the following result.

Corollary 1. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let e be a public exponent satisfying $e < N^{\frac{\sqrt{2}}{2}}$ and $ed_p = 1 + k_p(p-1)$ for some d_p with*

$$d_p < \frac{N^{\frac{\sqrt{2}}{4}}}{\sqrt{e}}.$$

Then N can be factored in polynomial time.

Proof. Starting with the equation $ed_p = 1 + k_p(p-1)$ with $e = N^\alpha$, $d_p = N^\delta$ and $p > N^{\frac{1}{2}}$, we get

$$k_p = \frac{ed_p - 1}{p-1} < \frac{ed_p}{p-1} < N^{\alpha+\delta-\frac{1}{2}}. \tag{3}$$

On the other hand, we have $ed_p \equiv 1 - k_p \pmod{p}$ with $d_p < N^\delta$ and

$$|1 - k_p| = k_p - 1 < k_p < N^{\alpha+\delta-\frac{1}{2}}.$$

To apply Theorem 4 with the equation $ex + y \equiv 0 \pmod{p}$ where $x = d_p < N^\delta$ and $y = k_p - 1 < N^{\alpha+\delta-\frac{1}{2}}$, the parameters α and δ must satisfy

$$\delta + \alpha + \delta - \frac{1}{2} \leq \frac{\sqrt{2}-1}{2}.$$

This leads to $\delta < \frac{1}{2}\left(\frac{\sqrt{2}}{2} - \alpha\right)$ and $d_p < N^\delta < \frac{N^{\frac{\sqrt{2}}{4}}}{\sqrt{e}}$. Observe that $\alpha + 2\delta < \frac{\sqrt{2}}{2}$. Plugging in (3), we get

$$k_p < N^{\alpha+\delta-\frac{1}{2}} < N^{\alpha+2\delta-\frac{1}{2}} < N^{\frac{\sqrt{2}}{2}-\frac{1}{2}} < q.$$

Hence, the parameters d_p and k_p are such that $ed_p + k_p - 1 = k_p p$ with $k_p \not\equiv 0 \pmod{q}$. Hence $ed_p - 1 + k_p \not\equiv 0 \pmod{N}$ which implies that the method of Theorem 4 will give the factorization of N in polynomial time. □

Notice that our attack on CRT-RSA works for exponents $e < N^{\frac{\sqrt{2}}{2}}$, that is when e is much smaller than N. This corresponds to a variant of RSA-CRT proposed by Galbraith, Heneghan and McKee [6] and to another variant proposed by Sun, Hinek and Wu [16]. We want to point out that our new attack improves Bleichenbacher and May's bound [1] where $d_p < \min\left\{\frac{1}{4}\left(\frac{N}{e}\right)^{\frac{2}{5}}, \frac{1}{3}N^{\frac{1}{4}}\right\}$ and $d_q < \min\left\{\frac{1}{4}\left(\frac{N}{e}\right)^{\frac{2}{5}}, \frac{1}{3}N^{\frac{1}{4}}\right\}$, that is when both d_p and d_q are suitably small. In other terms, our attack extends Bleichenbacher and May's attack in the sense that only d_p (or d_q) is small with $d_p < \frac{N^{\frac{\sqrt{2}}{4}}}{\sqrt{e}}$. On the other hand, the existing results on cryptanalysis of CRT-RSA will directly work on the CRT-RSA variant called Dual CRT-RSA. Consequently, our result improves the latest bounds on dual CRT-RSA obtained by Sarkar and Maitra [13].

Next, we consider an instance related to CRT-RSA when the public exponent e satisfies an equation $ex = y + z(p-1)$ with suitably small parameters x, y and z. We obtain the following result as a corollary of Theorem 4.

Corollary 2. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Suppose e is a public exponent satisfying $e < N$ and $ex = y + z(p-1)$ with*

$$x|z-y| < N^{\frac{\sqrt{2}-1}{2}} \text{ and } \gcd(z,q) = 1.$$

Then N can be factored in polynomial time.

Proof. Rewrite the equation $ex = y + z(p-1)$ as $ex + z - y = pz$. Assume that $\gcd(z,q) = 1$, $x < N^{\gamma}$ and $|z-y| < N^{\delta}$. Then, by Theorem 4, we can find the factorization of N in polynomial time if $\gamma + \delta \leq \frac{\sqrt{2}-1}{2}$, that is

$$x|z-y| < N^{\frac{\sqrt{2}-1}{2}},$$

which terminates the proof. □

5 Experimental Results

We have implemented the attack described in Section 4 using the algebra system Maple on a Intel(R) Core(TM)2 DUO CPU T5870 @ 2.00GHZ 2.00GHZ, 3.00Go RAM machine. Let us first present a detailed example.

5.1 A working example

We choose a 200-bit N which is a product of two 100-bit primes p and q satisfying $q < p < 2q$. We also choose a 100-bit e.

$$\begin{aligned} N &= 2746482122383906972393557363644983749146398460239422282612197, \\ e &= 1908717316858446782674807627631. \end{aligned}$$

We suppose that e satisfies $ed_p = 1 + k_p(p-1)$ with $d_p < \frac{N^{\frac{\sqrt{2}}{4}}}{\sqrt{e}}$. We rewrite this equation as $x_0 + ey_0 \equiv 0 \pmod{p}$ where $x_0 = k_p - 1$ and $y_0 = d_p$. Next, consider the polynomial $f(x,y) = x + ey$. We apply the lattice-based method of Herrmann and May with $m = 5$ and $t = 2$ as explained in Subsection 2.2. We find that the polynomials $h_1(x,y)$ and $h_2(x,y)$ share the common factor $407851x - 396114y$. Solving over the integers, this leads to the solution $(x_0, y_0) = (k_p - 1, d_p) = (396114, 407851)$. Hence $d_p = 407851 \approx N^{0.09}$ and $k_p = 396115 \approx N^{0.09}$. Using (k_p, d_p), one can find p, q as

$$\begin{aligned} p &= \gcd(ed_p + k_p - 1, N) = 1965268334695819089811552114253, \\ q &= \frac{N}{p} = 1397509985733832541423163654649. \end{aligned}$$

In connection with CRT-RSA, we observe that the private parameter d_q satisfying $ed_q \equiv 1 \pmod{(q-1)}$ is $d_q = 822446363998652526665788028903 \approx N^{0.49}$. This is greater than the bound $\min\left\{\frac{1}{4}\left(\frac{N}{e}\right)^{\frac{2}{5}}, \frac{1}{3}N^{\frac{1}{4}}\right\} \approx N^{0.2}$ obtained by Bleichenbacher and May in [1]. This shows that the technique of [1] will not work here.

5.2 Massive experiments

We generated 1000 RSA moduli $N = pq$ with 512-bit primes. For each modulus N, we generated a 512-bit exponent e such that $d_p < \frac{N^{\frac{\sqrt{2}}{4}}}{\sqrt{e}}$. The implementation was in all cases successful and it needs approximately 8 secondes to find the factors of the RSA modulus.

We also ran our experiments with random 1024-bit moduli $N = pq$ and various size of d_p as follows. We randomly select two distinct 512-bit primes p and q and a positive integer d_p of prescribed size such that $\gcd(d_p, (p-1)(q-1)) = 1$. The exponent e is then calculated as $e \equiv d_p^{-1} \pmod{(p-1)}$. Observe that e is of size approximately $N^{\frac{1}{2}}$, so that the condition connecting e and d_p becomes

$$d_p < \frac{N^{\frac{\sqrt{2}}{4}}}{\sqrt{e}} \approx N^{\frac{\sqrt{2}-1}{4}}.$$

Hence, for a 1024-bit modulus N, the CRT-exponent d_p is typically of size at most 110.

In Figure 2, we give the details of the computations using the method described in Subsection 2.2 with the lattice parameters $m = 4$ and $t = 2$.

Size of d_p	Size of e	Size of d_q	LLL execution time
10	511	510	5.35 sec
20	511	508	6.49 sec
40	511	508	6.49 sec
80	510	511	11.45 sec
90	510	510	11.80 sec
95	512	507	11.51 sec
100	511	511	11.74 sec
105	511	511	12.18 sec
110	502	511	11.06 sec

Fig. 2. Experimental results for various size of d_p.

6 Conclusion

In this paper, we presented a new attack on the RSA cryptosystem when the public key (N, e) satisfies an equation $ex + y \equiv 0 \pmod{p}$ with the constraint that $|x||y| < N^{\frac{\sqrt{2}-1}{2}}$. We showed that the number of such exponents with $e < N$ is at least $N^{\frac{\sqrt{2}}{2}-\varepsilon}$. As an application of our new attack, we presented the cryptanalysis of CRT-RSA if the private exponent d_p satisfies $d_p < \frac{N^{\frac{\sqrt{2}}{4}}}{\sqrt{e}}$ when p and q are of the same bit-size and e is much smaller than N. This improves the former result of Bleichenbacher and May for CRT-RSA with small CRT-exponents and balanced primes in the case that the public exponent e is significantly smaller than N.

References

1. Bleichenbacher, D. and 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.: A generalized Wiener attack on RSA. In Public Key Cryptography - PKC 2004, volume 2947 of Lecture Notes in Computer Science, pp. 1–13. Springer-Verlag (2004)
3. Boneh, D., Durfee, G.: Cryptanalysis of RSA with private key d less than $N^{0.292}$, Advances in Cryptology Eurocrypt'99, Lecture Notes in Computer Science Vol. 1592, Springer-Verlag, pp. 1–11 (1999)
4. Cohen, H.: A Course in Computational Number Theory, Graduate Texts in Mathematics, Springer (1993)
5. Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities. Journal of Cryptology, 10(4), pp. 233–260 (1997)
6. Galbraith, S.D., Heneghan, C. and J.F. McKee. Tunable balancing of RSA. In Proceedings of ACISP'05, volume 3574 of Lecture Notes in Computer Science, pp. pp. 280–292 (2005)
7. Hardy, G.H., Wright, E.M.: An Introduction to the Theory of Numbers. Oxford University Press, London (1965)
8. Hastad, J.: Solving simultaneous modular equations of low degree, SIAM J. of Computing, Vol. 17, pp. 336–341 (1988)
9. Herrmann, M. and May, A.: Solving linear equations modulo divisors: On factoring given any bits. J. Pieprzyk (Ed.): ASIACRYPT 2008, LNCS 5350, pp. 406–424 (2008)
10. Howgrave-Graham, N.: Finding small roots of univariate modular equations revisited, In Cryptography and Coding, LNCS 1355, Springer-Verlag, pp. 131–142 (1997)
11. Jochemsz, E. and 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)
12. Lenstra, A.K., Lenstra, H.W. and Lovász, L.: Factoring polynomials with rational coefficients, Mathematische Annalen, Vol. 261, pp. 513–534 (1982)
13. Maitra, M., Sarkar, S.: Cryptanalysis of Dual CRT-RSA, WCC 2011 - Workshop on Coding and Cryptography, pp. 27–36 (2011)
14. Quisquater, J.J. and Couvreur, C.: Fast decipherment algorithm for RSA public key cryptosystem. Electronic Letters, 18 (21): pp. 905–907, October (1982)
15. Rivest, R., Shamir, A., Adleman, L.: A Method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM, Vol. 21 (2), pp. 120–126 (1978)
16. Sun, H.-M., Hinek, M.J. and Wu, M.-E.: On the design of rebalanced CRT-RSA, Technical Report CACR 2005–35, University of Waterloo (2005)
17. Wiener, M.: Cryptanalysis of short RSA secret exponents, IEEE Transactions on Information Theory, Vol. 36, pp. 553–558 (1990)