CRYPTANALYSIS OF RSA WITH CONSTRAINED KEYS

Abderrahmane Nitaj

Département de mathématiques
Université de Caen
Boulevard Maréchal Juin
14032 Caen Cedex, France
nitaj@math.unicaen.fr

Abstract. Let $n = pq$ be an RSA modulus with unknown prime factors of equal bit-size. Let e be the public exponent and d be the secret exponent satisfying $ed \equiv 1 \pmod{\phi(n)}$ where $\phi(n)$ is the Euler totient function. To reduce the decryption time or the signature generation time, one might be tempted to use a small private exponent d. Unfortunately, in 1990, Wiener showed that private exponents smaller than $\frac{1}{3}n^{1/4}$ are insecure and in 1999, Boneh and Durfee improved the bound to $n^{0.292}$. In this paper we show that instances of RSA with even large private exponents can be efficiently broken if there exist positive integers X, Y such that $|eY - XF(u)|$ and Y are suitably small where F is a function of publicly known expression for which there exists an integer $u \neq 0$ satisfying $F(u) \approx n$ and pu or qu is computable from $F(u)$ and n. We show that the number of such exponents is at least $O\left(n^{3/4-\varepsilon}\right)$ when $F(u) = p(q-u)$.

1 Introduction

Let $n = pq$ be an RSA modulus, i.e the product of two large primes p, q of roughly the same size. Let e and d be the public and secret exponents satisfying $ed \equiv 1 \pmod{\phi(n)}$ where $\phi(n) = (p-1)(q-1)$ is the Euler totient function related to n. The public key and the private key consist of the tuples (n, e) and (p, q, d) respectively.

Since its publication in 1978, the RSA cryptosystem [8] has been analyzed for vulnerability by many researchers (see [2]). Since RSA is computationally expensive, one might be tempted to use short secret exponents d in order to speed up the decryption process. Unfortunately, in 1990, Wiener [11] showed that RSA is insecure if $d \leq \frac{1}{3}n^{\frac{1}{4}}$. In 2000, Boneh and Durfee [3] (heuristically) improved the bound to $d \leq n^{0.292}$. While

2000 *Mathematics Subject Classification.* 94A60, 11Y05.

Key words and phrases. RSA cryptosystem, Cryptanalysis, Continued fractions, Blömer-May attack, Coppersmith's algorithm.

Wiener's attack uses continued fractions, the Boneh and Durfee attack is based on Coppersmith's method for finding small roots of modular polynomial equations [4]. In 2002, de Weger [10] improved these bounds for the RSA modulus $n = pq$ with small prime difference $|p-q|$. Recently, Blömer and May [1] extended both Wiener and de Weger attacks for the RSA cryptosystems with secret exponents having the modular factorization $d \equiv -xy^{-1} \pmod{\phi(n)}$ where x and y are suitably small. Moreover, they showed that the number of such weak exponents is at least $O\left(n^{3/4-\varepsilon}\right)$ where ε is a positive constant.

All the known non-factoring attacks on RSA exploit the weakness of the public exponent e relative to $\phi(n)$ focusing on the information encoded in e and $\phi(n)$. The starting point is the equation

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

or, as considered in [1], the more general equation

$$ex + y = k\phi(n),$$

where x, y, k are suitably small relatively prime integers.

In this paper, we present an attack on RSA by exploiting additional information that may be encoded in the public exponent e relatively to special functions of the primes p and q. Let F be a function satisfying the conditions

$$\text{There exists an integer } u \neq 0 \text{ such that } F(u) \approx n. \tag{1}$$

$$\text{There exists a transformation relating } F(u) \text{ to a multiple of } p \text{ or } q. \tag{2}$$

We now introduce the concept of F-constrained public exponents. Let us formalize this notion.

Definition 1.1. *Let n be an RSA modulus and F a function satisfying the conditions (1), (2). A public exponent e is F-constrained if there exist an integer u and two coprime positive integers X and Y such that both Y and $|eY - F(u)X|$ are suitably small.*

The integers X, Y will be formally defined in Theorem 3.1. We list below typical examples of functions satisfying the conditions (1), (2). Let $u_0 \neq 0$ be a fixed rational and F a function defined by one of the following expressions

$$\begin{aligned}
F_1(u) &= p(q-u), && 1 \leq |u| < q.\\
F_1'(u) &= (p-u)q, && 1 \leq |u| < p.\\
F_2(u) &= n + u_0 - pu, && 1 \leq |u| < q + \frac{u_0}{p}.\\
F_2'(u) &= n + u_0 - qu, && 1 \leq |u| < p + \frac{u_0}{q}.\\
F_3(u) &= (q-u)\left(p - \frac{u_0}{u}\right), && 1 \leq |u| < q.\\
F_3'(u) &= (p-u)\left(q - \frac{u_0}{u}\right), && 1 \leq |u| < p.
\end{aligned}$$

Observe that when $u_0 = 1$, we have $F_3(1) = (p-1)(q-1) = \phi(n)$. This indicates that our method is a natural extension of the attack of Blömer and May [1] which in turn is an extension of Wiener's attack [11]. In this paper, we mainly study the cryptanalysis of RSA with F_1-constrained exponents. More precisely, we show that if e satisfies the equation

$$eY - F_1(u)X = Z \tag{3}$$

with unknown integers u, X, Y, Z such that

$$1 \le Y \le \frac{1}{2}\left(\frac{qF_1(u)}{e|u|}\right)^{\frac{1}{2}} \qquad \text{and} \qquad 1 \le |Z| \le \frac{2n^{-\frac{3}{4}}\,(n - p|u|)\,eY}{F_1(u)},$$

then n can be factored in polynomial time. In a new way, we will show that the number of F_1-constrained exponents is at least $O\left(n^{3/4-\varepsilon}\right)$.

Our new method works as follows. Assume that e is $F(u)$-constrained for some integer u where F is a function satisfying (1), (2). We use the continued fraction algorithm to find X and Y in (3) by replacing $\frac{e}{F(u)}$ by $\frac{e}{n}$. For every convergent $\frac{X}{Y}$ of the expansion, we compute the approximation $F(u) \approx \frac{eY}{X}$ and by (2), an approximation $\tilde{P}$ of a multiple of p or q. We then apply May's extension (Theorem 10 of [7]) of Coppersmith's method [4] to find the factorization of n.

The RSA cryptosystem and digital signature schemes are based on the generation of random primes p, q of roughly equal size and generation of random exponents e, d such that $ed \equiv 1 \pmod{\phi(pq)}$. Indeed, RSA with private exponent $d < n^{0.292}$, can be efficiently broken with Wiener's continued fraction attack [11] or Boneh and Durfee's lattice-based attack [3]. In this paper we show that there are some security risks if the public exponent is chosen poorly even if the companion private exponent is large. We recommend to avoid public exponents e satisfying $eY - F(u)X = Z$ with suitably small values X, Y, Z where F is a function of publicly known expression satisfying the conditions (1), (2). Notice that it is easy for a crypto-designer to see that the public exponent e is constrained by checking if $eY - F(u)X = Z$ is solvable in suitably small X, Y, Z for any function F in a fixed public list. On the other hand, our study shows that such exponents are numerous (at least $O\left(n^{3/4-\varepsilon}\right)$ with $F = F_1$).

The remainder of this paper is organized as follows. In Section 2 we review former continued fraction attacks on RSA with short secret exponents. In Section 3, we discuss the possibility of determining the first convergents of the continued fraction expansion of $\frac{e}{F(u)}$ using $\frac{e}{n}$ if e is $F(u)$-constrained. In Section 4 we show how to factor the RSA modulus n when e is F_1-constrained and give an estimation of the number of such exponents. We will use techniques from the continued fraction expansion combined with Coppersmith's Theorem [4] and May's extension [7]. In Section 5, we give a numerical example to illustrate our attack. Exploiting the symmetry on the primes p and q in F_1 and F_1', the vulnerability of an RSA cryptosystem with an F_1'-constrained public exponent e follows.

A key role in our attack is played by the following extension of the well-known theorem of Coppersmith [4].

Theorem 1.2. (May, Theorem 10 of [7]). *Let $n = pq$ be an RSA modulus with $q < p$. Let u be an (unknown) integer that is not a multiple of q. Suppose we know an approximation $\tilde{P}$ of pu with*

$$|pu - \tilde{P}| \leq 2n^{\frac{1}{4}}.$$

Then n can be factorized in time polynomial in $\log n$.

2 Former continued fraction attacks on RSA with weak exponents

In this section, we present three former attacks on RSA based on the continued fractions. All the attacks exploit the weakness of the public exponent e relative to $\phi(n)$.

2.1 The Wiener attack.

The public and private exponents are related by the equation $ed - k\phi(n) = 1$ rewritten as

$$\frac{e}{\phi(n)} - \frac{k}{d} = \frac{1}{\phi(n)d}.$$

Wiener exploits the fact that $\frac{e}{\phi(n)} \approx \frac{e}{n}$ and $n = pq$ for primes p, q of the same bit-size. Combining the arithmetical properties of $\phi(n)$ with the assumption $d < \frac{1}{3}n^{\frac{1}{4}}$, this leads to

$$\left|\frac{e}{n} - \frac{k}{d}\right| < \frac{1}{2d^2}.$$

By Legendre's theorem (see [6]), $\frac{k}{d}$ is a convergent of the continued fraction expansion of $\frac{e}{n}$.

2.2 The de Weger attack.

The continued fraction part of the de Weger attack [10] applies to an RSA modulus with small difference between its primes. It exploits the approximation $\phi(n) \approx n+1-2\sqrt{n}$ and the weakness of e relative to $\phi(n)$ and works as follows. Using $ed - k\phi(n) = 1$ and assuming that $\phi(n) > \frac{3}{4}n$, $n > 8d$ with

$$d < \frac{n^{\frac{3}{4}}}{p-q},$$

de Weger showed that

$$\left|\frac{e}{n+1-2\sqrt{n}} - \frac{k}{d}\right| < \frac{1}{2d^2}.$$

Hence $\frac{k}{d}$ is a convergent of the continued fraction expansion of $\frac{e}{n+1-2\sqrt{n}}$.

2.3 The Blömer-May attack.

The attack of Blömer and May [1] combines the continued fraction expansion of $\frac{e}{n}$ and Coppersmith's lattice-based technique for finding small roots of univariate modular polynomial equations [4]. The attack applies when the public exponent e is weak relative

to $\phi(n)$ and is based on the existence of coprime integers x, y, k satisfying $ex+y = k\phi(n)$ with

$$0 < x \leq \frac{1}{3}n^{\frac{1}{4}} \qquad \text{and} \qquad |y| \leq cn^{-\frac{3}{4}}ex,$$

where $c \leq 1$. Combining with the properties of $\phi(n)$, they showed that

$$\left|\frac{e}{n} - \frac{k}{x}\right| < \frac{1}{2x^2}.$$

Hence $\frac{k}{x}$ is a convergent of the continued fraction expansion of $\frac{e}{n}$. Next, they applied Coppersmith's method [4] to find the factorization of the modulus n as follows. Using $ex + y = k(n + 1 - p - q)$, we have

$$p + q = n + 1 - \frac{ex}{k} - \frac{y}{k}.$$

Since k and x are known, then $s = n+1-\frac{ex}{k}$ is an approximation of $p+q$ up to an error term $\frac{|y|}{k} \leq \frac{4}{3}cn^{\frac{1}{4}}$ (see [1] for more details). Let $t = \sqrt{s^2 - 4n}$. Then t is an approximation of $p - q$ up to an error term bounded by $9n^{\frac{1}{4}}$. This shows that $\frac{s+t}{2}$ is an approximation of p that can be bounded by $6n^{\frac{1}{4}}$. Applying Coppersmith's algorithm with $\frac{s+t}{2}$ gives the factorization of n.

The extension of the continued fraction attacks by Verheul and van Tilborg [9] and its modification by Dujella [5] applies to $d \leq n^{\frac{1}{4}+\frac{\gamma}{2}}$ provided exhaustive search on $O(\gamma \log_2(n))$ bits. These extensions are also based on the weakness of e relative to $\phi(n)$.

3 The continued fraction expansion of $\frac{e}{F(u)}$

Let F be a function satisfying (1), (2). Our goal in this section is to guess a part of the continued fraction expansion of $\frac{e}{F(u)}$. Recall that $F(u)$ is close to n for some unknown u. Moreover, we suppose that $0 < F(u) < 2n$ so that there exists α with $-\frac{1}{2} < \alpha < \frac{1}{2}$ such that

$$|F(u) - n| = n^{\frac{1}{2}+\alpha}. \tag{4}$$

Theorem 3.1. *Let F be a function satisfying (1), (2) and $n = pq$ an RSA modulus with $p < q$. Let u be an integer such that $|F(u) - n| = n^{\frac{1}{2}+\alpha}$, with $-\frac{1}{2} < \alpha < \frac{1}{2}$. Let X, Y, Z be coprime integers satisfying $eY - F(u)X = Z$. If*

$$Y < \frac{1}{2}n^{\frac{1}{4}-\frac{\alpha}{2}}\left(\frac{F(u)}{e}\right)^{\frac{1}{2}}, \tag{5}$$

and

$$|Z| \leq n^{\alpha-\frac{1}{2}}eY, \tag{6}$$

then $\frac{X}{Y}$ *is a convergent among the continued fraction expansion of* $\frac{e}{n}$.

Proof. Using $eY - F(u)X = Z$, we get

$$\begin{aligned}\left|\frac{e}{n} - \frac{X}{Y}\right| &\leq \left|\frac{e}{n} - \frac{e}{F(u)}\right| + \left|\frac{e}{F(u)} - \frac{X}{Y}\right| \\ &= \frac{e|F(u) - n|}{nF(u)} + \frac{|eY - F(u)X|}{F(u)Y} \\ &= \frac{en^{\alpha-\frac{1}{2}}}{F(u)} + \frac{|Z|}{F(u)Y}.\end{aligned}$$

Since $|Z| \leq n^{\alpha-\frac{1}{2}}eY$, then

$$\left|\frac{e}{n} - \frac{X}{Y}\right| \leq \frac{en^{\alpha-\frac{1}{2}}}{F(u)} + \frac{en^{\alpha-\frac{1}{2}}}{F(u)} = \frac{2en^{\alpha-\frac{1}{2}}}{F(u)}.$$

By assumption, we have

$$Y < \frac{1}{2}n^{\frac{1}{4}-\frac{\alpha}{2}}\left(\frac{F(u)}{e}\right)^{1/2},$$

Hence

$$\frac{2en^{\alpha-\frac{1}{2}}}{F(u)} < \frac{1}{2Y^2}.$$

which gives

$$\left|\frac{e}{n} - \frac{X}{Y}\right| < \frac{1}{2Y^2}.$$

By Legendre's theorem (see [6]), $\frac{X}{Y}$ is a convergent of the continued fraction expansion of $\frac{e}{n}$.

■

Theorem 3.1 relates the unknowns Y, Z in the equation (3). Let us find a lower bound for the quantity X.

Corollary 3.2. *With the hypothesis of Theorem 3.1, we have*

$$X \geq \left(1 - n^{\alpha-\frac{1}{2}}\right)\frac{eY}{F(u)}. \tag{7}$$

Proof. Since by assumption $-\frac{1}{2} < \alpha < \frac{1}{2}$, then $-1 < \alpha - \frac{1}{2} < 0$. Hence $1 - n^{\alpha-\frac{1}{2}} > 0$. Combining $Z = eY - F(u)X$ and $|Z| \leq n^{\alpha-\frac{1}{2}}eY$, we get

$$X = \frac{eY - Z}{F(u)} \geq \frac{eY - |Z|}{F(u)} = \frac{eY}{F(u)}\left(1 - \frac{|Z|}{eY}\right) \geq \frac{eY}{F(u)}\left(1 - n^{\alpha-\frac{1}{2}}\right),$$

which terminates the proof.

■

4. Vulnerability of RSA using $F = F_1$

In this section, we will show that using an RSA modulus $n = pq$ with $q < p$ and an F_1-constrained public exponent e is insecure. Recall that $F_1(u) = p(q-u)$. We will also give an estimation of the number of $F_1(u)$-constrained exponents for a fixed u and derive an estimation of the number of F_1-constrained exponents.

4.1 Cryptanalysis of RSA with F_1-constrained exponents.

Theorem 3.1 relates the unknowns Y, Z of the equation (3) and shows that the first convergents of $\frac{e}{F_1(u)}$ are among the convergents of $\frac{e}{n}$. In the following theorem, we give a condition relating X and Y and leading to the factorization of n.

Theorem 4.1. *Let X, Y be coprime positive integers. If there exists an integer u with $1 \leq |u| \leq q-1$ such that $|eY - F_1(u)X| \leq 2n^{\frac{1}{4}}X$, then n can be factored in polynomial time.*

Proof. Put $Z = eY - F_1(u)X$. Using $F_1(u) = p(q-u)$, we get

$$pu = n - \frac{eY}{X} + \frac{Z}{X}.$$

Let $\tilde{P} = n - \frac{eY}{X}$. We have

$$\left|\tilde{P} - pu\right| = \frac{|Z|}{X} \leq \frac{2n^{\frac{1}{4}}X}{X} = 2n^{\frac{1}{4}}.$$

Hence $\tilde{P}$ is an approximation of pu with an error term less than $2n^{\frac{1}{4}}$. We conclude the proof by applying Theorem 1.2.

■

Let us consider the α term as defined in (4). Since $q < \sqrt{n} < p$ and $F_1(u) = p(q-u) = n - pu$ with $1 \leq |u| \leq q-1$ we get $|F_1(u) - n| = p|u| = n^{\frac{1}{2}+\alpha}$ with $0 < \alpha < \frac{1}{2}$.

We now state our result concerning the vulnerability of RSA using $F = F_1$.

Theorem 4.2. *Let $n = pq$ be an RSA modulus with $q < p$ and u an integer satisfying $1 \leq |u| \leq q-1$ and $p|u| = n^{\frac{1}{2}+\alpha}$. Let X, Y be coprime positive integers. If X and Y satisfy $eY - F_1(u)X = Z$, with*

$$Y < \frac{1}{2}n^{\frac{1}{4}-\frac{\alpha}{2}}\left(\frac{F_1(u)}{e}\right)^{\frac{1}{2}}, \tag{8}$$

and

$$|Z| \leq \frac{2n^{\frac{1}{4}}\left(1 - n^{\alpha-\frac{1}{2}}\right)eY}{F_1(u)}, \tag{9}$$

then $\frac{X}{Y}$ is a convergent of $\frac{e}{n}$ and n can be factored in polynomial time.

Proof. Let us first show that $\frac{X}{Y}$ is a convergent of $\frac{e}{n}$. Observe that Y satisfies the inequality (5) of Theorem 3.1 with $F = F_1$. Let $Z = eY - F_1(u)X$. Assume that Z satisfies (9). Since $F_1(u) \geq n - n^{\frac{1}{2}+\alpha}$, we get

$$|Z| \leq \frac{2n^{\frac{1}{4}}\left(1 - n^{\alpha-\frac{1}{2}}\right)eY}{F_1(u)} \leq \frac{2n^{\frac{1}{4}}\left(1 - n^{\alpha-\frac{1}{2}}\right)eY}{n - n^{\frac{1}{2}+\alpha}} = 2n^{-\frac{3}{4}}eY \leq n^{\alpha-\frac{1}{2}}eY.$$

This shows that (6) is also satisfied. Hence, by Theorem 3.1, $\frac{X}{Y}$ is a convergent of $\frac{e}{n}$. On the other hand, combining (7) with $F = F_1$ and (9), we get

$$\frac{|Z|}{X} \leq \frac{|Z|F_1(u)}{\left(1 - n^{\alpha-\frac{1}{2}}\right)eY} \leq 2n^{\frac{1}{4}}.$$

Hence, by Theorem 4.1, n can be factored in polynomial time.

■

4.2 The number of $F_1(u)$-constrained exponents.

Let u be a fixed integer satisfying $1 \leq |u| \leq q - 1$. We indicate below how the crypto designer could build public exponents which are $F_1(u)$-constrained using only very short values of X, Y. We begin by the following useful lemma. We use the usual notation $\lfloor x \rfloor$ for the integral part of x.

Lemma 4.3. *Let $n = pq$ be an RSA modulus with $q < p$ and u an integer satisfying $1 \leq |u| \leq q - 1$ and $p|u| = n^{\frac{1}{2}+\alpha}$. Let X, Y be coprime integers with*

$$1 \leq X \leq Y < \frac{1}{2}n^{\frac{1}{4}-\frac{\alpha}{2}}.$$

If $e = \left\lfloor F_1(u)\frac{X}{Y} \right\rfloor$, then $e > n^{\frac{1}{2}-\alpha}$.

Proof. Let $Z = eY - F_1(u)X$. By the definition of e, we have

$$0 \leq F_1(u)\frac{X}{Y} - e < 1.$$

Combining with the inequalities $1 \leq X < Y < \frac{1}{2}n^{\frac{1}{4}-\frac{\alpha}{2}}$, this gives us

$$e + 1 > F_1(u)\frac{X}{Y} \geq (n - p|u|)\frac{1}{Y} > 2\,(n - p|u|)\,n^{\frac{\alpha}{2}-\frac{1}{4}}.$$

To show that $e > n^{\frac{1}{2}-\alpha}$, it suffices to show that

$$2\,(n - p|u|)\,n^{\frac{\alpha}{2}-\frac{1}{4}} > n^{\frac{1}{2}-\alpha} + 1. \tag{10}$$

Note that $p|u| = n^{\frac{1}{2}+\alpha}$. Then $n^{\alpha} = p|u|n^{-\frac{1}{2}}$ and consequently

$$n^{\frac{\alpha}{2}-\frac{1}{4}} = p^{\frac{1}{2}}|u|^{\frac{1}{2}}n^{-\frac{1}{4}}n^{-\frac{1}{4}} = \left(\frac{|u|}{q}\right)^{\frac{1}{2}}.$$

Similarly,

$$n^{\frac{1}{2}-\alpha} = n^{\frac{1}{2}}p^{-1}|u|^{-1}n^{\frac{1}{2}} = \frac{q}{|u|}.$$

Hence (10) is equivalent with

$$2\left(n - p|u|\right)\left(\frac{|u|}{q}\right)^{\frac{1}{2}} > \frac{q}{|u|} + 1.$$

Let

$$f(u) = 2\left(n - p|u|\right)\left(\frac{|u|}{q}\right)^{\frac{1}{2}} - \frac{q}{|u|} - 1,$$

with $1 \leq |u| \leq q-1$. An arithmetical study of the derivatives of f shows that for any such u we have

$$f(u) \geq \min(f(1), f(q-1)) = f(q-1) = 2p\left(\frac{q-1}{q}\right)^{\frac{1}{2}} - \frac{q}{q-1} - 1 > 0.$$

This confirms (10) and completes the proof.

■

Corollary 4.4. *Let $n = pq$ be an RSA modulus with $q < p$ and u an integer satisfying $1 \leq |u| \leq q-1$ and $p|u| = n^{\frac{1}{2}+\alpha}$. Let X, Y be coprime integers with*

$$1 \leq X \leq Y < \frac{1}{2}n^{\frac{1}{4}-\frac{\alpha}{2}}.$$

If $e = \left\lfloor F_1(u)\frac{X}{Y}\right\rfloor$, then $\frac{X}{Y}$ is a convergent of both $\frac{e}{F_1(u)}$ and $\frac{e}{n}$ and e is $F_1(u)$-constrained.

Proof. Let $Z = eY - F_1(u)X$. Since $1 \leq |u| \leq q-1$, $p > \sqrt{n}$ and $1 \leq X \leq Y < \frac{1}{2}n^{\frac{1}{4}-\frac{\alpha}{2}}$, then

$$F_1(u) = n - pu \geq n - p|u| \geq n - p(q-1) = p > n^{\frac{1}{2}} > 2Y^2.$$

On the other hand, by the definition of e, we have

$$0 \leq F_1(u)\frac{X}{Y} - e < 1. \tag{11}$$

Hence

$$\left|\frac{e}{F_1(u)} - \frac{X}{Y}\right| < \frac{1}{F_1(u)} < \frac{1}{2Y^2}.$$

This shows that $\frac{X}{Y}$ is a convergent of $\frac{e}{F_1(u)}$. Let us show that $\frac{X}{Y}$ is a convergent of $\frac{e}{n}$. By (11) and Lemma 4.3 we have

$$|Z| = |eY - F_1(u)X| < Y < n^{\alpha-\frac{1}{2}}eY,$$

and the inequality (6) of Theorem 3.1 is satisfied where $F = F_1$. Moreover, by (11), we have

$$\frac{F_1(u)}{e} \geq \frac{Y}{X} \geq 1.$$

Combining with $Y < \frac{1}{2}n^{\frac{1}{4}-\frac{\alpha}{2}}$, this gives

$$Y < \frac{1}{2}n^{\frac{1}{4}-\frac{\alpha}{2}}\left(\frac{F_1(u)}{e}\right)^{\frac{1}{2}},$$

and (5) is also satisfied with $F = F_1$. Hence, by Theorem 3.1, $\frac{X}{Y}$ is a convergent of $\frac{e}{n}$. Finally, using (11), we have

$$\frac{|Z|}{X} = \frac{|eY - F_1(u)X|}{X} < \frac{Y}{X} \leq Y < \frac{1}{2}n^{\frac{1}{4}-\frac{\alpha}{2}} < 2n^{\frac{1}{4}}.$$

Thus, by Theorem 4.1, e is $F_1(u)$-constrained which terminates the proof.

■

Corollary 4.4 indicates that every couple (X, Y) of coprime positive integers with $1 \leq X < Y < \frac{1}{2}n^{\frac{1}{4}-\frac{\alpha}{2}}$ and every integer u with $1 \leq |u| \leq q-1$ yield a candidate public exponent e for which the RSA cryptosystem is insecure. We show below that different couples produce different candidate public exponents.

Lemma 4.5. *Let $n = pq$ be an RSA modulus with $q < p$ and u an integer satisfying $1 \leq |u| \leq q-1$ and $p|u| = n^{\frac{1}{2}+\alpha}$ with $0 < \alpha < \frac{1}{2}$. Let X, X', Y and Y' be positive integers with $\gcd(X, Y) = \gcd(X', Y') = 1$ and*

$$1 \leq X \leq Y < \frac{1}{2}n^{\frac{1}{4}-\frac{\alpha}{2}} \qquad \text{and} \qquad 1 \leq X' < Y' < \frac{1}{2}n^{\frac{1}{4}-\frac{\alpha}{2}}.$$

Let $e = \left\lfloor F_1(u)\frac{X}{Y} \right\rfloor$ and $e' = \left\lfloor F_1(u)\frac{X'}{Y'} \right\rfloor$. If $e = e'$, then $(X, Y) = (X', Y')$.

Proof. Without loss of generality, suppose that $\frac{X}{Y} \geq \frac{X'}{Y'}$. By definition, e satisfies (11). Similarly, we have

$$0 \leq F_1(u)\frac{X'}{Y'} - e' < 1. \tag{12}$$

Combining (11) and (12), we get

$$\left(\frac{X}{Y} - \frac{X'}{Y'}\right)F_1(u) - 1 < e - e' < \left(\frac{X}{Y} - \frac{X'}{Y'}\right)F_1(u) + 1.$$

From this, we derive

$$0 \leq \left(\frac{X}{Y} - \frac{X'}{Y'}\right) F_1(u) < e - e' + 1.$$

By assumption $e = e'$. Then $0 \leq \left(\frac{X}{Y} - \frac{X'}{Y'}\right) F_1(u) < 1$ or equivalently,

$$0 \leq (XY' - YX')F_1(u) < YY'.$$

Combining the inequalities $1 \leq Y < \frac{1}{2}n^{\frac{1}{4}-\frac{\alpha}{2}}$, $1 \leq Y' < \frac{1}{2}n^{\frac{1}{4}-\frac{\alpha}{2}}$ and $F_1(u) \geq n - p|u| \geq n - p(q-1) = p > n^{\frac{1}{2}}$, we get

$$0 \leq (XY' - X'Y) < \frac{YY'}{F_1(u)} < \frac{\frac{1}{4}n^{\frac{1}{2}-\alpha}}{n^{\frac{1}{2}}} < 1.$$

Hence $XY' - X'Y = 0$ and since $\gcd(X, Y) = \gcd(X', Y') = 1$, we get $X = X'$ and $Y = Y'$.

■

For a fixed integer u satisfying $1 \leq |u| \leq q - 1$, we state below a lower bound for the number of $F_1(u)$-constrained public exponents.

Theorem 4.6. *Let $n = pq$ be an RSA modulus with $q < p$ and u an integer satisfying $1 \leq |u| \leq q - 1$ and $p|u| = n^{\frac{1}{2}+\alpha}$. The number of $F_1(u)$-constrained public exponents is at least $O\left(n^{\frac{3}{4}-\alpha-\varepsilon}\right)$.*

Proof. Let ε be a positive constant and u a fixed integer with $1 \leq |u| \leq q-1$. Let X and Y be coprime positive integers satisfying $1 \leq X \leq Y < \frac{1}{2}n^{\frac{1}{4}-\frac{\alpha}{2}-\varepsilon}$. Define $e = \left\lfloor F_1(u)\frac{X}{Y} \right\rfloor$ and $Z = eY - F_1(u)X$. Using similar arguments as in the proof of Corollary 4.4, we get $\frac{|Z|}{X} < 2n^{\frac{1}{4}-\varepsilon}$. If $\gcd(e, \phi(n)) \neq 1$, then e is not a valid public exponent. Let $e' = e + h$ for some integer h with $\gcd(e + h, \phi(n)) = 1$ and

$$1 \leq h \leq n^{\frac{1}{4}}\frac{X}{Y}.$$

Let $Z' = e'Y - F_1(u)X$. Since $Z < 0$, then

$$\frac{|Z'|}{X} = \frac{|(e+h)Y - F_1(u)X|}{X} = \frac{|Z + hY|}{X} \leq \frac{\max(|Z|, hY)}{X} < n^{\frac{1}{4}}.$$

Hence, by Theorem 4.1, e' is $F_1(u)$-constrained. This shows that every couple (X, Y) satisfying $\gcd(X, Y) = 1$ builds approximately $\frac{1}{2}n^{\frac{1}{4}}\frac{X}{Y}$ public exponents which are $F_1(u)$-constrained. Hence, the number of such exponents depends on the number of couples (X, Y) satisfying $\gcd(X, Y) = 1$ and $1 \leq X \leq Y < n^{\frac{1}{4}-\frac{\alpha}{2}-\varepsilon}$. For a fixed Y, there are

$\phi(Y)$ positive integers X such that $\gcd(X,Y)=1$ and $1 \le X \le Y$. Let $m = \left\lfloor \frac{1}{2} n^{\frac{1}{4}-\frac{\alpha}{2}-\varepsilon} \right\rfloor$. Using the well known estimation

$$\phi(Y) \ge \frac{KY}{\log\log(Y)} \ge \frac{KY}{\log\log(n)} = Y n^{-\varepsilon'},$$

where K is a constant related to the Euler constant, the number of the $F_1(u)$-constrained exponents is at least

$$\sum_{1 \le X \le Y \le m} \frac{1}{2} n^{\frac{1}{4}} \frac{X}{Y} \phi(Y) \ge \sum_{X=1}^{m} \frac{1}{2} n^{\frac{1}{4}-\varepsilon'} X = n^{\frac{1}{4}-\varepsilon'} \frac{m(m+1)}{4} = O\left(n^{\frac{3}{4}-\alpha-2\varepsilon-\varepsilon'}\right).$$

Replacing $2\varepsilon + \varepsilon'$ by ε, this terminates the proof.

■

4.3 The number of F_1-constrained exponents.

Theorem 4.6 gives an estimation of the number of $F_1(u)$-constrained exponents for a fixed u. It remains to give an estimation of the number of F_1-constrained exponents. Let u and u' be a fixed integers with $1 \le |u|, |u'| \le q-1$. We show below that if e is simultaneously constrained to $F_1(u)$ and $F_1(u')$, then $u = u'$.

Lemma 4.7. *Let $n = pq$ be an RSA modulus with $q < p$ and let u, u' be integers satisfying $1 \le |u|, |u'| \le q-1$ and $p|u| = n^{\frac{1}{2}+\alpha}$, $p|u'| = n^{\frac{1}{2}+\alpha'}$. Let X, Y, X', Y' be positive integers satisfying $\gcd(X,Y) = \gcd(X',Y') = 1$, and*

$$1 \le X \le Y < \frac{1}{2} n^{\frac{1}{4}-\frac{\alpha}{2}} \qquad \text{and} \qquad 1 \le X' < Y' < \frac{1}{2} n^{\frac{1}{4}-\frac{\alpha'}{2}}.$$

Let $e = \left\lfloor F_1(u)\frac{X}{Y} \right\rfloor$ and $e' = \left\lfloor F_1(u')\frac{X'}{Y'} \right\rfloor$. If $e = e'$ then $u = u'$ and $(X,Y) = (X',Y')$.

Proof. Assume that

$$e = \left\lfloor F_1(u)\frac{X}{Y} \right\rfloor = e' = \left\lfloor F_1(u')\frac{X'}{Y'} \right\rfloor.$$

From this, we get

$$\left| F_1(u)\frac{X}{Y} - F_1(u')\frac{X'}{Y'} \right| < 1.$$

Using $F_1(u) = n - pu$, $F_1(u') = n - pu'$, this gives

$$|(q-u)XY' - (q-u')X'Y| < \frac{YY'}{p}.$$

Since by assumption $1 \le X \le Y < \frac{1}{2} n^{\frac{1}{4}-\frac{\alpha}{2}}$, $1 \le X' < Y' < \frac{1}{2} n^{\frac{1}{4}-\frac{\alpha'}{2}}$ and $p > \sqrt{n}$, then

$$|(q-u)XY' - (q-u')X'Y| < \frac{YY'}{p} < \frac{1}{4} n^{\frac{1}{4}-\frac{\alpha}{2}+\frac{1}{4}-\frac{\alpha'}{2}-\frac{1}{2}} = \frac{1}{4} n^{-\frac{\alpha+\alpha'}{2}} < 1.$$

Since $(q-u)XY' - (q-u')X'Y$ is an integer, then $(q-u)XY' - (q-u')X'Y = 0$ and consequently $(q-u)XY' = (q-u')X'Y$. Set $g = \gcd(q-u, q-u')$. Then

$$\frac{q-u}{g}XY' = \frac{q-u'}{g}X'Y$$

Further, $\gcd((q-u)/g, (q-u')/g) = \gcd(X,Y) = \gcd(X',Y') = 1$. From this, it follows that

$$X = \frac{q-u'}{g}X', \quad Y = \frac{q-u}{g}Y', \quad X' = \frac{q-u}{g}X, \quad Y' = \frac{q-u'}{g}Y.$$

Combining X and X', we get

$$X = \frac{q-u'}{g}X' = \frac{q-u'}{g}\frac{q-u}{g}X$$

and $\frac{q-u'}{g}\frac{q-u}{g} = 1$. Hence $\frac{q-u'}{g} = \frac{q-u}{g} = 1$ and $u = u'$. Finally, by Lemma 4.5, we obtain $(X,Y) = (X',Y')$ which terminates the proof.

■

We now give an estimation for the number of F_1-constrained public exponents.

Theorem 4.8. *Let $n = pq$ be an RSA modulus with $q < p < 2q$. The number of F_1-constrained public exponents is at least $O\left(n^{\frac{3}{4}-\varepsilon}\right)$.*

Proof. By Theorem 4.6, for every u with $1 \leq |u| \leq q-1$ and $p|u| = n^{\frac{1}{2}+\alpha}$, the number of the $F_1(u)$-constrained exponents is at least $O\left(n^{\frac{3}{4}-\alpha-\varepsilon}\right)$. Hence, the number of the F_1-constrained exponents is at least

$$N(F_1) = \sum_{0<\alpha<1} n^{\frac{3}{4}-\alpha-\varepsilon}.$$

Since $q < p < 2q$, then $n < p^2 < 2n$ and $p < 2^{\frac{1}{2}}n^{\frac{1}{2}}$. Combining this with $n^{\alpha} = n^{-\frac{1}{2}}p|u|$, we get

$$n^{-\alpha} = n^{\frac{1}{2}}p^{-1}|u|^{-1} > 2^{-\frac{1}{2}}|u|^{-1}.$$

It follows that

$$N(F_1) = n^{\frac{3}{4}-\varepsilon}\sum_{\alpha} n^{-\alpha} > 2^{-\frac{1}{2}}n^{\frac{3}{4}-\varepsilon}\sum_{|u|=1}^{q-1}|u|^{-1}.$$

The sum $\sum_{|u|=1}^{q-1}|u|^{-1}$ is related to the harmonic series $\sum_{u=1}^{\infty}u^{-1}$ which diverges. Trivially, we have

$$\sum_{|u|=1}^{q-1}|u|^{-1} > 2$$

and finally

$$N(F_1) \geq 2^{\frac{1}{2}}n^{\frac{3}{4}-\varepsilon},$$

which terminates the proof.

■

5. A numerical example using $F = F_1$

Let $n = pq$ be an RSA modulus with $q < p$. Let e be a public exponent. In this section, we give an algorithm to factor the modulus n if e is $F_1(u)$-constrained for some unknown u where $F_1(u) = p(q-u)$.

The algorithm.

INPUT: a) The RSA modulus $n = pq$ with unknown prime factors.

b) The public exponent e such that $eY - F(u)X = Z$ for some unknown integers

u, X, Y and Z satisfying (8) and (9).

1. Compute the continued fraction expansion of $\frac{e}{n}$.
2. For every convergent $\frac{X}{Y}$ such that $Y < \frac{1}{2}n^{\frac{1}{4}}$:
   i) Compute $\tilde{P} = n - \frac{eX}{Y}$.
   ii) Apply Coppersmith's algorithm with $\tilde{P}$ and output a value N.
   iii) Compute $g = \gcd(N, n)$. If $g \neq n$ then stop.

OUTPUT: $p = g$, $q = \frac{n}{p}$, $u = \frac{N}{p}$.

Let us now consider the 48 digit example.

$$n = 941096252089784462564816358283310787682673275523,$$
$$e = 315625340556173340571223891244486052970403822 67.$$

The first 24 partial quotients of the continued fraction expansion of $\frac{e}{n}$ are

$$[0,\ 29,\ 1,\ 4,\ 2,\ 5,\ 1,\ 7\ 1,\ 12,\ 14,\ 2,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 5,\ 2,\ 3020,\ 1, 1,\ ...].$$

The 21th convergent is $\frac{X}{Y} = \frac{78754791}{2348222057}$. With $\tilde{P} = n - \frac{eY}{X}$, Coppersmith's algorithm outputs $N = -16844161339196881321690656 75$. This gives $p = \gcd(N, n) = 13211106932703436330737 77$, $u = \frac{N}{p} = -1271$, $q = \frac{n}{p} = 712352308465649934350899$, and the factorization of n is achieved.

We are now able to analyze our attack and the Blömer-May attack. The attack of Blömer and May gives the factorization of n if the prime factors p and q satisfy $|n + 1 - \frac{ex}{k} - p - q| < n^{\frac{1}{4}}$ for some convergent $\frac{k}{x}$ of $\frac{e}{n}$ or $\frac{e}{n+1-2\sqrt{n}}$. No such convergent exists which explains why Blömer-May's attack fails. Our attack succeeds since there exist an integer $u = -1271$ and a convergent $\frac{X}{Y} = \frac{78754791}{2348222057}$ of $\frac{e}{n}$ such that (8) and (9) are satisfied.

The secret exponent is $d = 56521469710136555875801528913954880304529539 5763$ and satisfies $d \approx n^{0.995\cdots} > \frac{1}{3}n^{\frac{1}{4}}$ which explains why the original attack of Wiener [11] fails. Similarly, we have $d > \frac{n^{3/4}}{p-q}$, which explains why the continued fraction attack of de Weger [10] also fails.

6. Conclusion

Using methods based on continued fractions and May's extension of Coppersmith's Theorem, we showed that an RSA cryptosystem with modulus $n = pq$ and a public exponent e is insecure if there exist an integer u such that $n - pu \approx n$ and a convergent $\frac{X}{Y}$ of $\frac{e}{n}$ for which both $|eY - (n - pu)X|$ and Y are relatively small. Moreover we showed that there are at least $O\left(n^{\frac{3}{4}-\varepsilon}\right)$ public exponents making the cryptosystem insecure.

We analysed the security of RSA using the function F_1 where $F_1(u) = p(q - u)$. The situation is similar with the symmetric function F_1' where $F_1'(u) = q(p-u)$. As mentioned in the introduction, RSA could be insecure if the public exponent e is constrained with other sort of functions satisfying similar conditions. Our results show that one should be very cautious when using an RSA modulus with a constrained exponent.

References

1. J. Blömer, A. May, *A generalized Wiener attack on RSA*, In Practice and Theory in Public Key Cryptography (PKC 2004), Lecture Notes in Computer Science, Springer-Verlag **2947** (2004), 1–13.
2. D. Boneh, *Twenty years of attacks on the RSA cryptosystem*, Notices of the American Mathematical Society (AMS) **46 (2)** (1999), 203–213.
3. D. Boneh, G. Durfee, *Cryptanalysis of RSA with private exponent d less than* $N^{0.292}$, IEEE Transactions on Information Theory **46** (2000), 1339–1349.
4. D. Coppersmith, *Small solutions to polynomial equations and low exponent vulnerabilities*, Journal of Cryptology **10 (4)** (1997), 223–260.
5. A. Dujella, *Continued fractions and RSA with small secret exponent*, Tatra Mt. Math. Publ. **29** (2004), 101–112.
6. S. Lang, *Introduction to diophantine approximations*, Addison-Wesley Pub. Co, (1966).
7. A. May, *New RSA Vulnerabilities Using Lattice Reduction Methods*, PhD thesis, University of Paderborn, (2003), `http://wwwcs.upb.de/cs/ag-bloemer/personen/alex/publications/`.
8. R.L. Rivest, A. Shamir, L. Adleman, *A method for obtaining digital signatures and public-exponent cryptosystems*, Communications of the ACM, **21** (1978), 120–126.
9. E. Verheul, H. van Tilborg, *Cryptanalysis of less short RSA secret exponents*, Appl. Algebra Eng. Commun. Comput. **8** (1997), 425–435.
10. B. de Weger, *Cryptanalysis of RSA with small prime difference*, Appl. Algebra Eng. Commun. Comput. **13** (2002), 17–28.
11. M. Wiener, *Cryptanalysis of short RSA secret exponents*, IEEE Transactions on Information Theory **36** (1990), 553-558.