ASM Sc. J., 12, Special Issue 5, 2019 for ICoAIMS2019, 143-149

# The Blömer-May's Weak Key Revisited

R.R.M. Tahir[1], M.A. Asbullah[1,2*] and M.R.K. Ariffin[1,3]

[1]*Institute for Mathematical Research, Universiti Putra Malaysia, Malaysia*

[2]*Centre of Foundation Studies for Agricultural Science, Universiti Putra Malaysia, Malaysia*

[3]*Department of Mathematics, Faculty of Science, Universiti Putra Malaysia, Malaysia*

Blömer-May's attack is notable cryptanalysis towards RSA cryptosystem, which can be viewed as an extension of the Wiener's attack such that focused on its generalized for of key equation. Note that the said attack can lead a polynomial-time factorization of modulus $N$ via continued fraction method. Later, the attack was reformulated to satisfies $xy < \frac{N}{4(p+q)}$. In this paper, we propose an improved bound of Blömer-May's generalized key exponents that satisfies $xy < \frac{3(p+q)N}{2((p-q)N^{\frac{1}{4}}+(p+q)^2)}$. We show that our result is marginally better than the previous study.

**Keywords:** RSA cryptosystem; cryptanalysis; weak key; generalized key equation; continued fraction.

## I. INTRODUCTION

The RSA cryptosystem (Rivest *et al.*, 1978) has a global-wide use as a public key cryptosystem in the communication and banking fields. The strength of this cryptosystem is based on its integer factorization on a modulus $N = pq$ where $p$ and $q$ are the prime numbers. Since then, it inspired many researchers to design public-key cryptosystems based on integer factorization problems such as Asbullah *et al.* (2018), Asbullah and Ariffin (2016) and Mahad *et al.* (2017). Focussed on the RSA design, there is public key $e$ satisfies a specific Diophantine equation $ed = 1 + k\phi(N)$, which also knwon as the RSA key equation, where $d$ is a private exponent and $\phi(N)$ is the Euler totient function (Abu Bakar *et al.*, 2017). The private exponent $d$ alongside with several other parameters such as $p$, $q$, and $\phi(N)$ must be kept the covert from the public. Therefore, the study on finding the limitation of RSA was started from the 1980s, especially on the factorization of modulus $N$ until recent publications such as Abu Bakar *et al.* (2018), Gafar *et al.* (2018) and Rahman *et al.* (2018).

Historically, since the 1990s, the small private exponents had paid attention on RSA key generation. Wiener (1990) particularly introduced an attack on small private exponents. In the analysis of small private exponents, Wiener (1990) proved that if $d < \frac{1}{3}N^{\frac{1}{4}}$, then modulus $N$ can factor in polynomial time via continued fraction method. Later, Nitaj (2013) improved the upper bound satisfying $d < \frac{\sqrt{6\sqrt{2}}}{6}N^{\frac{1}{4}}$. Recently, another proof to Wiener's short secret exponent satisfying $d < \frac{1}{2}N^{\frac{1}{4}}$ (Asbullah & Ariffin, 2019). Blömer and May (2004) introduced an attack which extend from Wiener (1990) attack by proposing an RSA variant key equation where a public key $e$ satisfies $ex = z + y\phi(N)$, with $0 < x < \frac{1}{3}\sqrt{\frac{\phi(N)}{e}\frac{N^{\frac{3}{4}}}{p-q}}$ and $|z| < \frac{p-q}{\phi(N)N^{\frac{1}{4}}}ex$. The attack is focused on the Diophantine equation problem which is solvable by continued fraction expansion and by Coppersmith's method obtaining the prime factors of the modulus $N$.

Nitaj (2013) revisited the Blömer-May's attack and reformulate the attack which considering the case of unbalanced prime $p$ and $q$. By using Blömer-May's key equation, the key exponents in Nitaj (2013) satisfy $xy < \frac{N}{4(p-q)}$ with $|z| < \frac{p-q}{3(p+q)}N^{\frac{1}{4}}y$. The work of Nitaj (2013) can be viewed as a reformulation of the attack via generalized key exponents, which had given the motivation to this study; i.e. to revisit the study with the aims to improve the generalized key exponents. Thus, we present another proof of Blömer-May's attack which improve the bound of

*Corresponding author's e-mail: ma_asyraf@upm.edu.my generalized key equation where $xy < \frac{3(p+q)N}{2((p-q)N^{\frac{1}{4}}+3(p+q)^2)}$. As a result, a new bound which shows some significant improvement as compared as result provided in Nitaj (2013).

In this paper, there are four sections which are organized sequentially. In Section 2, existing yet important theorems and previous results were presented which will be used in this study. Next section presents the improved generalized key exponents bound, followed with a working algorithm and numerical example. In Section 4, we compared the result with the previous study. Finally, the conclusion in Section 5.

## II. PRELIMINARIES

This section presents the fundamental technique of the continued fraction expansion and also the useful existing results that will be utilized throughout this paper.

### *A. Continued Fraction*

Let $r$ be a real number which has unique continued fraction expansion,

$$r = [a_0, a_1, a_2, \dots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\dots}}}$$

where we define the sequence $\{r_k\}$ and $\{a_k\}$ recursively with

$$r = r_0, a_k = \lfloor r_k \rfloor, r_{k+1} = \frac{1}{r_k - a_k}, \text{for} k \geq 0$$

The elements $a_0, a_1, a_2, \dots$ are called partial quotients with $a_0 \in \mathbb{Z}$ and $a_1, a_2, \dots \in \mathbb{Z}^+$. The value $r$ be a finite number if $r = [a_0, a_1, a_2, \dots, a_i]$ for $0 \leq i \leq k$ and be the convergents to the rational numbers $\frac{p_i}{q_i}$ satisfying

$$\frac{p_i}{q_i} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_i}}}}$$

The following theorem is one of the important results related to continued fraction expansion and known as the Legendre's theorem. This theorem was widely used for cryptanalytical results such as Asbullah *et al.* (2016) and Asbullah and Ariffin (2016).

**Theorem 1** (Asbullah *et al.*, 2016) *Let* $\frac{y}{x} = [a_0, a_1, a_2, \dots]$ *be a continued fraction expansion of* $r$. *If* $x$ *and* $y$ *are coprime integers such that*

$$\left| r - \frac{y}{x} \right| < \frac{1}{2x^2},$$

*then* $\frac{y}{x}$ *is one of the convergents in continued fraction expansion of* $r$.

### *B. Coppersmith's Method*

A method for finding small roots of univariate polynomial equation $f(x_0) \equiv 0 \pmod N$ was introduced by Coppersmith (1997). This method is useful for many applications especially in cryptanalysis on RSA cryptosystem. In this study, there is a partial knowledge prime $p$ is known in which the bound difference of approximation $p$ is at most $N^{\frac{1}{4}}$. Thus, we recall a theorem that can be used for factorization of $N$.

**Theorem 2** (Coppersmith, 1997) *Let* $N = pq$ *be RSA Modulus with* $q < p < 2q$. *Suppose we know the most significant bit of one of the prime in* $N$ *with*

$$|p - \rho| < N^{\frac{1}{4}}$$

*then the modulus* $N$ *can be factored in polynomial time.*

### *C. Previous Result*

Blömer and May (2004) had study about the variant RSA key equation $ex - \phi(N)y = z$ with small parameter of $x$, $y$, and $z$ that can factorise modulus $N$ as shown in the following theorems.

**Theorem 3** (Blömer & May, 2004) *Suppose* $(N, e)$ *is an RSA public key and the key equation* $ex - \phi(N)y = z$ *is satisfied by the public exponent* $e$ *with*

$$0 < x < \frac{1}{3}\sqrt{\frac{\phi(N)}{e}\frac{N^{\frac{3}{4}}}{p-q}} \text{ and } |z| < \frac{p-q}{\phi(N)N^{\frac{1}{4}}}ex$$

Then, Nitaj (2013) revisited the variant key equation to determine an polynomials time factorisation of modulus $N$ as following theorem.

**Theorem 4** (Nitaj, 2013) *Suppose $(N, e)$ is an RSA public key and the key equation $ex - \phi(N)y = z$ is satisfied by the public exponent $e$ with*

$$xy < \frac{N}{4(p+q)} \text{and} |z| < \frac{p-q}{3(p+q)}N^{\frac{1}{4}}y$$

*Then, the polynomials time factorisation of modulus N can be occured.*

Then, there are three lemmas that engage in this study (see (Nitaj, 2008)). For the first lemma, consider the primes $p$ and $q$ have same bit size, as follows.

**Lemma 1** (Nitaj, 2008) *Let $N = pq$ be an RSA Modulus with $q < p < 2q$. Then,*

$$\frac{\sqrt{N}}{\sqrt{2}} < q < \sqrt{N} < p < \sqrt{2}\sqrt{N}.$$

Then, the inequalities for $p + q$ and $p - q$ based on Lemma 1 as lemma follows.

**Lemma 2** (Nitaj, 2008) *Let RSA modulus $N = pq$ with balanced prime $q < p < 2q$. Then*

$$2\sqrt{N} < p + q < \frac{3}{\sqrt{2}}\sqrt{N} \text{and} \frac{\sqrt{N}}{\sqrt{2}} < p - q < \sqrt{N}.$$

The next lemma presents the factorisation of modulus $N$ occured when there is the approximation of $p + q$.

**Lemma 3** (Nitaj, 2013) *Let RSA modulus $N = pq$ with balanced prime $q < p < 2q$. Given an approximation of $p + q$ with at most $\frac{p-q}{3(p+q)}N^{\frac{1}{4}}$ , then, the polynomials time factorisation of modulus $N$ can be occured.*

## III. RESULTS AND DISCUSSION

This section presents the improved result on bound of generalized key exponents, which compared it with Nitaj's bound $xy < \frac{N}{4(p+q)}$ (Nitaj, 2013) as follows.

**Proposition 1** *Let $N = pq$ with an RSA public key $(N, e)$ and $q < p < 2q$. Suppose that e satisfies a key equation $ex - y\phi(N) = z$ with gcd $(x, y)$=1 and*

$$xy < \frac{3(p+q)N}{2((p-q)N^{\frac{1}{4}} + 3(p+q)^2)} \text{and} |z| < \frac{p-q}{3(p+q)}N^{\frac{1}{4}}y$$

*then, $\frac{y}{x}$ is amongst the convergence of the continued fraction $\frac{e}{N}$.*

*Proof.* Consider the generalized key equation $ex - y\phi(N) = z$ and then derive the following equation;

$$ex - y\phi(N) = z$$
$$ex - y(N + 1 - (p + q)) = z$$
$$ex - yN = z - (p + q - 1)y \quad (1)$$

Multiply (1) with $\frac{1}{Nx}$ into yields

$$\left|\frac{e}{N} - \frac{y}{x}\right| = \frac{|z - y(p + q - 1)|}{Nx}$$
$$\leq \frac{|z| + y(p+q-1)}{Nx} \quad (2)$$

Observed the numerator on right hand side of (2). Suppose $|z| < \frac{p-q}{3(p+q)}N^{\frac{1}{4}}y$ and gcd $(x, y)$=1. Hence,

$$|z| + y(p + q - 1) < \frac{p-q}{3(p+q)}N^{\frac{1}{4}}y + y(p + q - 1)$$
$$< \frac{p-q}{3(p+q)}N^{\frac{1}{4}}y + y(p + q)$$
$$= \left(\frac{(p-q)N^{\frac{1}{4}} + 3(p+q)(p+q)}{3(p+q)}\right)y$$
$$= \left(\frac{(p-q)N^{\frac{1}{4}} + 3(p+q)^2}{3(p+q)}\right)y \quad (3)$$

Substituting (3) in (2) will give

$$\left|\frac{e}{N}-\frac{y}{x}\right| < \frac{\left(\frac{(p-q)N^{\frac{1}{4}}+3(p+q)^2}{3(p+q)}\right)y}{Nx}$$

$$= \frac{\left((p-q)N^{\frac{1}{4}}+3(p+q)^2\right)y}{3(p+q)Nx} \qquad (4)$$

Assuming $xy < \frac{3(p+q)N}{2((p-q)N^{\frac{1}{4}}+3(p+q)^2)}$, then

$$xy < \frac{3(p+q)N}{2((p-q)N^{\frac{1}{4}}+3(p+q)^2)}$$

$$\frac{2((p-q)N^{\frac{1}{4}}+3(p+q)^2)}{3(p+q)N} < \frac{1}{xy}$$

$$\frac{((p-q)N^{\frac{1}{4}}+3(p+q)^2)y}{3(p+q)N} < \frac{x}{x}\cdot\frac{1}{2x}$$

$$\frac{((p-q)N^{\frac{1}{4}}+3(p+q)^2)y}{3(p+q)Nx} < \frac{1}{2x^2}$$

By continued fraction computation and Theorem 1 implies that $\frac{y}{x}$ is a convergent of the fraction of $\frac{e}{N}$ (i.e. (4) which is less than $\frac{1}{2x^2}$). Follows Lemma 3 to factor the modulus $N$, hence the approximation of $p+q$ can be define the following proposition.

**Proposition 2** *Let $x$ and $y$ found from the list of the computed continued fraction $\frac{e}{N}$. Let $T$ be the approximation of $p+q$ where $T = N+1-\frac{ex}{y}$. Then, factorisation of modulus N can be occured in polynomials time.*

*Proof.* Suppose $x$ and $y$ are yields from the convergent of continued fraction expansion of $\frac{e}{N}$. Then, from Blömer-May's key equation, we get

$$ex - y\phi(N) = z$$

$$ex - y(N-(p+q)+1) = z$$

$$\frac{ex}{y} - N + (p+q) - 1 = \frac{z}{y}$$

$$p+q-\left(N+1-\frac{ex}{y}\right) = \frac{z}{y}$$

Let $T = N+1-\frac{ex}{y}$ . Using $|z| < \frac{|p-q|}{3(p+q)}N^{\frac{1}{4}}y$ from Proposition 1, then

$$\left|p+q-\left(N+1-\frac{ex}{y}\right)\right| = |p+q-T| = \frac{|z|}{y}$$

$$< \frac{\frac{|p-q|}{3(p+q)}N^{\frac{1}{4}}y}{y}$$

$$= \frac{|p-q|}{3(p+q)}N^{\frac{1}{4}} (5)$$

From (5) the approximation of $p+q$ is computed through $T = N+1-\frac{ex}{y}$. By Lemma 3, if an approximation of $p+q$ is upper-bounded by $\frac{|p-q|}{3(p+q)}N^{\frac{1}{4}}$, then the factorisation of modulus $N$ can be occured in polynomials time. Therefore, we show the workflow algorithm on Algorithm 1 on factor modulus $N$ based on Proposition 1 and Proposition 2.

**Algorithm 1.** Factoring algorithm of the modulus $N$ via Proposition 1 and Proposition 2.

```
Input: Public key $(e,N)$
Output: prime $p$ and $q$
  i.   Compute the continued fraction $\frac{e}{N}$.
  ii.  For every convergents of $\frac{e}{N}$ denoted by $\frac{y'}{x'}$,
       compute $T = N+1-\frac{ex'}{y'}$.
  iii. Applying Lemma 3 with $T, e$ and $N$.
  iv.  Output the prime factors $p$ and $q$.
  v.   Else, repeat (ii)
```

The above Algorithm 1 is actually the factoring algorithm of the modulus $N$ using the results of Proposition 1 and Proposition 2, respectively. The input is the public key $(e,N)$. Observe that the Step (2) will execute the continued fraction expansion of $\frac{e}{N}$. Hence, each fraction among the list of the convergent are possible candidate of $x$ and $y$ satisfying $ex - y\phi(N) = z$ . For each candidate will be assigned as $x'$and $y'$. For every $\frac{y'}{x'}$, the approximation $p+q$ namely $T$ will be computed such as $T = N+1-\frac{ex'}{y'}$. and approximation $p$, $\rho = \frac{T+\sqrt{T^2-4N}}{2}$. By Lemma 3, if the value of $T$ is upper-bounded by $\frac{|p-q|}{3(p+q)}N^{\frac{1}{4}}$, then the factorisation of modulus $N$ can be occured in polynomials time. If the factorization of modulus $N$ is success, then the Algorithm 3 will output $p$ and $q$, which are the correct factorisation of the modulus $N$. Otherwise, the Algorithm 1 need to repeat with the next candidate of $\frac{y'}{x'}$. The following is a numerical example in order to demonstrate the proposed algorithm.

**Example 1.** *Given the modulus $N = 9550583597402242457$ and public exponent $e = 153613565783535$. By continued fraction compuation, the list of $\frac{y}{x}$ is listed as follows.*

$$\left[\cdots\frac{33}{2051702},\frac{80}{4973823},\frac{113}{7025525},\frac{532}{33075923},\cdots\right]$$

Observe that $\frac{113}{7025525}$ as a candidate of convergent $\frac{e}{N}$.

*Then we compute $T = 6228564597$. We undergo Lemma 3 with $N$ and $T$, then we get the prime $p = 3499211623$ and its correspending $q = \frac{N}{p} = 2729352959$ thus, corresponding to Algorithm 3, we got $y = y' = 113$ and $x = x' = 7025525$.*

Let us compare the bound of generalized key exponents, by applying the same problem into Nitaj's attacks. According to Example 1, the product of $x$ and $y$ obtained is $xy = 793884325$ which is larger than and Nitaj's bound (i.e $xy < \frac{N}{4(p+q)} = 383338066$). Thus, the given example has covered the Nitaj's bound.

## IV. COMPARATIVE ANALYSIS

We recall Nitaj's bound to compare with our work. Thus, by the following proving, we show our bound deduce in term of modulus $N$ supported by Lemma 1. We start our proving with

$$xy < \frac{3(p+q)N}{2((p-q)N^{\frac{1}{4}} + 3(p+q)^2)}$$

Based on Lemma 2, suppose $\frac{\sqrt{N}}{\sqrt{2}} < p - q$ and get

$$\begin{aligned}
\frac{3(p+q)N}{2((p-q)N^{\frac{1}{4}}+3(p+q)^2)} &< \frac{3(p+q)N}{2\left(\frac{\sqrt{N}}{\sqrt{2}}N^{\frac{1}{4}}+3(2\sqrt{N})^2\right)} \\
&= \frac{3(p+q)N}{2\left(\frac{\sqrt{N}}{\sqrt{2}}N^{\frac{1}{4}}+12N\right)} \\
&< \frac{3(\frac{3}{\sqrt{2}}\sqrt{N})N}{2\left(\frac{\sqrt{N}}{\sqrt{2}}N^{\frac{1}{4}}+12N\right)} \\
&= \frac{3(\frac{3}{\sqrt{2}}\sqrt{N})N}{2\left(\frac{N^{\frac{3}{4}}}{\sqrt{2}}+12N\right)} \\
&= \frac{9N^{\frac{3}{2}}}{2\sqrt{2}(N^{\frac{3}{4}})\left(\frac{1}{\sqrt{2}}+12N\right)} \\
&= \frac{9N^{\frac{3}{4}}}{2\sqrt{2}(\frac{1}{\sqrt{2}}+12N^{\frac{1}{4}})} \\
&< \frac{9N^{\frac{3}{4}}}{2\sqrt{2}(12N^{\frac{1}{4}})} \\
&= \frac{9}{24\sqrt{2}}\sqrt{N} \approx 0.265\sqrt{N}
\end{aligned}$$

Thus we get the size $xy$ is about $\frac{9}{24\sqrt{2}}\sqrt{N}$ or approximately $0.265\sqrt{N}$. For Nitaj, the size we get via parameter $N$ is

$$\begin{aligned}
xy &< \frac{N}{4(p+q)} \\
&< \frac{N}{4(2\sqrt{N})} \\
&= \frac{1}{8}\sqrt{N} \approx 0.125\sqrt{N}
\end{aligned}$$

As previously stated, we revisit Blömer - May's attack with its variant key equation which then the attack is reformulated by Nitaj. We only compare our bound with Nitaj's bound since both bound have the generalized key exponents $xy$; unlike Blömer-May's bound that has only key exponent $x$. Thus, we recall Nitaj's and ours bound to be compared to this section. In this case, we have derived our bound to make it have the same term as Nitaj's bound. The result is shown in Table 1.

Table 1. The Comparison of Generalized Key Exponent's Bound $xy$

| Reference | Bound of Key Exponents $xy$ |
|---|---|
| (Nitaj, 2013) | $0.125\sqrt{N}$ |
| Proposed Bound | $0.265\sqrt{N}$ |

Our aim in this study is to improve the bound generalized key exponents of Nitaj's revisited bound from Blömer - May attack. By the observation from Table 1, our bound give is positively improved from the previous bound. Our bound enhances the Nitaj's bound by $0.14\sqrt{N}$, thus, our bound is can attack more size of generalized key exponents than Nitaj (2013).

## V. CONCLUSION

Blömer and May (2004) had extended Wiener's attack to create one of notable attack in RSA cryptosystem where there is a public key $e$ satisfies a generalized key equation $ex + \phi(N)y = z$ with certain condition $x$ and $z$. Their attack was revisited by Nitaj which reformulating the generalized key exponents $xy < \frac{N}{4(p+q)}$ and $|z| < \frac{p-q}{3(p+q)}N^{\frac{1}{4}}y$ . We introduced another proof of bound generalized key exponents for $xy < \frac{3(p+q)N}{2((p-q)N^{\frac{1}{4}}+3(p+q)^2)}$ which give a positive result on extending the Nitaj's revisit attack.

## VI. ACKNOWLEDGEMENT

The present research was partially supported by the Putra Grant - GP/2017/9552200.

## VII. REFEREENCES

Abubakar, S.I., Ariffin, M.R.K., & Asbullah, M.A. 2018, 'A new simultaneous diophantine attack upon RSA moduli $N = pq$', *Proceedings of the 6th International Cryptology and Information Security Conference 2018, CRYPTOLOGY 2018*, pp. 119-138.

Asbullah, M. A., & Ariffin, M. R. K. 2019. 'Another Proof Of Wiener's Short Secret Exponent', *Malaysian Journal of Science, MJS*, pp. 62-68.

Asbullah, M.A., Ariffin, M.R.K., & Mahad, Z. 2018, 'Enhanced AA$_β$ Cryptosystem: The design', *Proceedings of the 6th International Cryptology and Information Security Conference 2018*, CRYPTOLOGY 2018, pp. 94 -102 .

Asbullah, M.A., Ariffin, M.R.K., & Mahad, Z. 2016, 'Analysis on the Rabin-p Cryptosystem', *AIP Conference Proceedings*, vol. 1787, pp 080012.

Asbullah, M.A., & Ariffin, M.R.K. 2016, 'Analysis on the AA$_β$ Cryptosystem', *Proceedings of the 5th International Cryptology and Information Security Conference 2016, CRYPTOLOGY 2016*, pp. 41 – 48 .

Asbullah, M. A., & Ariffin, M. R. K. 2016. 'Design of Rabin-like cryptosystem without decryption failure.' *Malaysian Journal of Mathematical Sciences, MJMS*, vol. 10, pp. 1 – 18.

Blömer, J., & May, A. 2004, 'A generalized Wiener attack on RSA', *In International Workshop on Public Key Cryptography*, Springer, Berlin, Heidelberg, pp. 1-13.

Coppersmith, D. 1997, 'Small solutions to polynomial equation and low exponent RSA vulnerabilities'. *Journal of Cryptology*, p. 233-260.

Ghafar, A.H.A., Ariffin, M.R.K., & Asbullah, M.A. 2018. 'Extending pollard class of factorable RSA modulus', *Proceedings of the 6th International Cryptology and Information Security Conference 2018*, *CRYPTOLOGY 2018*, pp. 103 -118.

Mahad, Z., Asbullah, M.A., & Ariffin, M.R.K. 2017, 'Efficient methods to overcome Rabin cryptosystem decryption failure', *Malaysian Journal of Mathematical Sciences*, vol. 11, no. S2, pp. 9-20.

Nitaj, A. 2008, 'Another generalization of Wiener's attack on RSA', *In International Conference on Cryptology in Africa*, pp. 174-190.

Nitaj, A. 2013. 'Diophantine and lattice cryptanalysis of the RSA cryptosystem', *In Artificial Intelligence, Evolutionary Computing and Metaheuristics, Springer, Berlin, Heidelberg*, pp. 139-168.

Rahman, N.N.A., Ariffin, M.R.K., Asbullah, M.A., & Yunos, F. 2018. 'New vulnerability on system of $N_i = p_i^2 q_i$ using good approximation of ϕ(N) ', *Proceedings of the 6th International Cryptology and Information Security Conference 2018, CRYPTOLOGY 2018*, pp. 139-150.

Rivest, R.L., Shamir, A., & Adleman, L. 1978. 'A Method for Obtaining Digital Signatures and Public

- Key Cryptosystems', *Communications of the ACM*, vol. 21, no. 2, pp.120-126.

Wiener, M. J. 1990. 'Cryptanalysis of short RSA secret exponents', *IEEE Transactions on Information theory*, vol. 36, pp. 553-558.