Weak Keys in RSA over The Work of Blomer & May

Navaneet Ojha and Sahdeo Padhye
(Corresponding author: Sahdeo Padhye)

Department of Mathematics, Motilal Nehru National Institute Of Technology, Allahabad-211004 (UP), India.
(Email: sahadeo_mathrsu@yahoo.com)

(Received May 18, 2010; revised and accepted Aug. 16 & Nov. 14, 2010)

Abstract

In this paper we generalize the idea given by Weger and Maitra & Sarkar. This generalization is coming from the concept of $x9.31-1997$ standard for public key cryptography, Section 4.1.2, i.e., *there are a number of recommendations for the generalization of the primes of an RSA modulus. Among them, the ratio of the primes shall not be close to the ratio of small integers.* Also we try to improve the range of weak keys of RSA cryptosystem for the Generalized Wiener's attack given by Blomer & May. We have shown that the range of weak keys can be extended by more than 8 times than the range given by Blomer & May. Further we have shown that for $|ap - bq| \leq N^{\frac{\alpha}{2}}$ where $0 < \alpha \leq 1$, if e satisfies an equation $ex + y = m\phi(N)$, for $m > 0$. Then N can be factored in(O poly$(\log N)$) times when $0 < x \leq \frac{1}{6}\sqrt{\frac{\phi(N)}{e}}N^{\frac{1}{2}-\frac{\alpha}{4}}$ and $|y| \leq \frac{|ap-bq|}{\phi(N)N^{1/4}}ex$.

Keywords: Continued fractions, coppersmith's method, RSA, Wiener's attack

1 Introduction

The RSA cryptosystem [8, 9] invented by Rivest, Shamir and Adleman in 1978 is one of the most practical and popular public key cryptosystem in the history of the cryptology. The security of RSA depends on mainly two primes p, q of the same bit size and the integer d satisfying $ed \equiv 1 \bmod \phi(N)$, where $N = pq$ and $(e, \phi(N)) = 1$. The key pair (e, N) is called RSA public key. The integer N is called RSA modulus. The integers e and d are called encryption (public) key and decryption (secret) key exponent respectively. To reduce the decryption time, one may wish to use short secret exponent d. This was cryptanalyzed ed by Wiener [11] in 1990 who observed that RSA is insecure if $d < \frac{1}{3}N^{\frac{1}{4}}$. More precisely, he showed that every public exponent $e \in Z^*_{\phi(N)}$ which corresponds to the secrete exponent $d < \frac{1}{3}N^{\frac{1}{4}}$, yields the factorization of the modulus in time polynomial in $log(N)$. Wiener's method is based on the continued fractions. In 1999, Boneh & Durfee [2] improved Wiener's bound to $d < N^{0.292}$ using lattice reduction technique [3, 6]. In 2000, Weger [10] improved Wiener's bound to $d < N^{\delta}$, where $\delta < \frac{3}{4} - \beta$ and assuming that $\phi(N) > \frac{3}{4}(N)$ where N is, with a small difference between its prime factors $p - q = N^{\beta}$, $\frac{1}{4} \leq \beta \leq \frac{1}{2}$. A fast RSA-variant that makes use of special RSA-keys was proposed by Yen et al. [12]in 2001 which is known as YKLM scheme. Due to large decryption exponent d, the Wiener and the Boneh & Durfee attack can not directly be applied to this variants. In 2004, Blomer and May [1] generalized Wiener [11] and Weger [10] attacks by showing that N can be factorized in polynomial time, when the public exponent e satisfies an equation $ex + y = 0 \bmod \phi(N)$ with $0 < x \leq \frac{1}{3}\sqrt{\frac{\phi(N}{e}}$ $\frac{N^{\frac{3}{4}}}{p-q}$ and $|y| \leq \frac{p-q}{\phi(N)N^{\frac{1}{4}}}ex$. In fact, the Blomer & May attack is applicable in YKLM scheme also. In their article [1] Blomer & May introduce the notion of *weak keys* in RSA first time. They defined the *weak keys* as: there are classes of public keys (N, e) where every element in the class yields the factorization of N. In the case of the Wiener attack the class consists of all public key tuples (N, e) where $ed - 1 \equiv 0 mod \phi(N)$ with $d < \frac{1}{3}N^{\frac{1}{4}}$. In 2008, Maitra and Sarkar [7] generalized the range of weak keys given by Blomer & May to the public exponent e satisfies an equation $ex + y = m\phi(N)$, for $m > 0$ with $0 < x \leq \frac{1}{6}\sqrt{\frac{\phi(N}{e}}$ $N^{\frac{1}{2}-\frac{\gamma}{2}}$ and $|y| \leq \frac{N^{\gamma}}{\phi(N)N^{\frac{1}{4}}}ex$, where $|\rho q - p| \leq N^{\gamma}$, $\gamma \leq \frac{1}{2}$ and ρ $(1 \leq \rho \leq 2)$ is known to the attacker. They have shown that the class of weak keys identified in [1] can be extended by more than 5 times. In this paper, we present new class of weak keys in RSA by extending the rage of weak keys by 8 time given in [1] and 1.5 times given in [7]. Also, In this paper, we present an extension of Generalized Wiener attack given by Blomer & May [1] and the attack given by Maitra & Sarkar [7]. Our method combines the Continued fractions & Coppersmith's method. Our approach is more efficient if $\frac{p}{q}$ is close to $\frac{a}{b}$ with small integers a and b. This is a step in the direction of the $X9.31 - 1997$ standard for PKC (Section 4.12) which requires that the ratio of the primes shall not be close to the ratio of small integers. Instead of

considering $|\rho q - p| \leq N^{\gamma}$, assuming a and b is known to the attacker, here we consider $|ap - bq| \leq \frac{1}{16}N^{\frac{\alpha}{2}}$, where $0 < \alpha \leq 1$, and a, b is coming from the concept of $\frac{p}{q}$ shall not be close to the ratio of small integers. Here a & b have the same bit length. Also a is coprime to b, $a > b$. We can generate the value of a and b by Stern-Brocot Tree [4].

Rest of the sections are as follows. Second section is a preliminary section where we present the continued fraction and Coppersmith's method. Section three is our main part of the article where we present a class of new weak keys in RSA by proving that N can be factored in (O poly$(\log N)$) times when $0 < x \leq \frac{1}{6}\sqrt{\frac{\phi(N)}{e}}N^{\frac{1}{2}-\frac{\alpha}{4}}$ and $|y| \leq \frac{|ap-bq|}{\phi(N)N^{1/4}}ex$. Finally we conclude our article in Section 4.

2 Preliminaries

Continued Fraction: The continued fraction [5] expansion of a real number:

$$\xi = a_o + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + ...}}}$$

where $a_o \epsilon Z$ and $a_i \epsilon N - \{O\}$ for $i \geq 1$. The numbers $a_0, a_1, a_2, ..$ are called the partial quotients. In short we can write $\xi = [a_0, a_1, ...]$. For $i \geq 0$,the rationales $\frac{p_i}{q_i} = [a_0, a_1, ...a_i]$ are called the convergent of the continued fraction expansion of ξ. If $\xi = \frac{a}{b}$ is rational with $gcd(a, b) = 1$, then the continued fraction expansion is finite and the continued fraction algorithm finds the convergent in time $O((\log b)^2)$.

Coppersmith's method[3]: At Eurocrypt1996, Coppersmith [3] introduced two lattice reduction based techniques to find small roots of polynomial diophantine equations. The first technique works for modular univariate polynomials, the second for bivariate integer polynomial equations. He illustrated his technique for solving bivariate integer polynomial equations with the problem of finding the factors of $N = pq$ if we are given the high order $\frac{1}{4}\log_2 N$ bits of q.

Theorem 1. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Given an approximation $\tilde{p}$ of p with $|p - \tilde{p}| < N^{\frac{1}{4}}$, then N can be factories time polynomial in $\log N$.*

3 New Weak keys in RSA

Let us we begin this section with the following proposition.

Proposition 1. *Let $|ap - bq| \leq \frac{1}{16}N^{\frac{\alpha}{2}}$, where $a \leq b \leq 2a$, and $0 < \alpha \leq 1$. Then $|p + q - (\sqrt{\frac{b}{a}} + \frac{1}{\sqrt{\frac{b}{a}}})\sqrt{N}| < \frac{1}{8}N^{\frac{\alpha}{2}}$.*

Proof. Since

$$|ap - bq| \leq \frac{1}{16}N^{\frac{\alpha}{2}}. \quad (1)$$

On multiplying p, we get

$$\begin{aligned} |ap^2 - bpq| &\leq p\frac{1}{16}N^{\frac{\alpha}{2}} \\ \Rightarrow |p + \sqrt{\frac{b}{a}}\sqrt{N}||p - \sqrt{\frac{b}{a}}\sqrt{N}| &\leq p\frac{1}{16a}N^{\frac{\alpha}{2}} \\ \Rightarrow |1 + \frac{\sqrt{\frac{b}{a}N}}{p}||p - \sqrt{\frac{b}{a}}\sqrt{N}| &\leq \frac{1}{16a}N^{\frac{\alpha}{2}} \\ \Rightarrow |p - \sqrt{\frac{b}{a}}\sqrt{N}| &< \frac{1}{16a}N^{\frac{\alpha}{2}} < \frac{1}{16}N^{\frac{\alpha}{2}} \\ & (as\ |1 + \frac{\sqrt{\frac{b}{a}N}}{p}| > 1). \end{aligned}$$

Similarly, on multiplying q on both sides in Inequality (1), we have

$$\begin{aligned} |apq - bq^2| &\leq q\frac{1}{16}N^{\frac{\alpha}{2}} \\ \Rightarrow |aN - bq^2| &\leq q\frac{1}{16}N^{\frac{\alpha}{2}} \\ \Rightarrow |N - \frac{b}{a}q^2| &\leq q\frac{1}{16a}N^{\frac{\alpha}{2}} \\ \Rightarrow |\sqrt{\frac{b}{a}}q - \sqrt{N}||\sqrt{\frac{b}{a}}q + \sqrt{N}| &\leq q\frac{1}{16a}N^{\frac{\alpha}{2}} \end{aligned}$$

Since $|\sqrt{\frac{b}{a}} + \frac{\sqrt{N}}{q}| > 1$, as $\frac{b}{a} \geq 1$, finally we have

$$|q - \sqrt{\frac{N}{\frac{b}{a}}}| < \frac{1}{16\sqrt{ab}}N^{\frac{\alpha}{2}} < \frac{1}{16}N^{\frac{\alpha}{2}}$$

Hence $|p+q-(\sqrt{\frac{b}{a}}+\frac{1}{\sqrt{\frac{b}{a}}})\sqrt{N}| \leq |p-\sqrt{\frac{b}{a}N}|+|q-\sqrt{\frac{N}{\frac{b}{a}}}| < \frac{1}{8}N^{\frac{\alpha}{2}}$. □

Theorem 2. *Let $|ap - bq| \leq \frac{1}{16}N^{\frac{\alpha}{2}}$, with a and b be small integers and $0 < \alpha \leq 1$, and $d = N^{\delta}$. Then N can be factored in $O(poly(\log N))$ time when $\delta < \frac{1}{2} - \frac{\alpha}{4}$.*

Proof. We know that if $|ap - bq| \leq \frac{1}{16}N^{\frac{\alpha}{2}}$, then

$$\begin{aligned} |p + q - (\sqrt{\frac{b}{a}} + \frac{1}{\sqrt{\frac{b}{a}}})\sqrt{N}| &< \frac{1}{8}N^{\frac{\alpha}{2}} \\ \Rightarrow |\phi(N) - N - 1 + (\sqrt{\frac{b}{a}} + \frac{1}{\sqrt{\frac{b}{a}}})\sqrt{N}| &< \frac{1}{8}N^{\frac{\alpha}{2}} \end{aligned}$$

Now, if $ed-1=k\phi(N)$, then

$$\begin{aligned}
&|\frac{e}{N-(\sqrt{\frac{b}{a}}+\frac{1}{\sqrt{\frac{b}{a}}})\sqrt{N}+1}-\frac{k}{d}|\\
\leq\ &|\frac{e}{N-(\sqrt{\frac{b}{a}}+\frac{1}{\sqrt{\frac{b}{a}}})\sqrt{N}+1}-\frac{e}{\phi(N)}|+|\frac{e}{\phi(N)}-\frac{k}{d}|\\
<\ &\frac{|\phi(N)-(N-(\sqrt{b/a}+\frac{1}{\sqrt{b/a}}\sqrt{N}+1)|}{N-(\sqrt{b/a}+\frac{1}{\sqrt{b/a}})\sqrt{N}+1}+\frac{1}{d(\phi(N)}\\
<\ &\frac{1}{4}N^{\frac{\alpha}{2}-1}+\frac{1}{4d^2},
\end{aligned}$$

on assuming $N-(\sqrt{b/a}+\frac{1}{\sqrt{b/a}})\sqrt{N}+1>\frac{N}{2}$ and $\phi(N)>4d$. When $\frac{N^{\frac{\alpha}{2}-1}}{4}<\frac{1}{4d^2}$, then

$$|\frac{e}{N-(\sqrt{\frac{b}{a}}+\frac{1}{\sqrt{\frac{b}{a}}})\sqrt{N}+1}-\frac{k}{d}| \ < \ \frac{1}{2d^2}$$

Therefore by the *Legendre theorem*, $\frac{k}{d}$ is one of the convergent of the continued fraction of $\frac{e}{N-(\sqrt{b/a}+\frac{1}{\sqrt{b/a}})\sqrt{N}+1}$.

Now, by setting $d=N^{\delta}$ in the inequality $\frac{N^{\frac{\alpha}{2}-1}}{4}<\frac{1}{4d^2}$, we get $\delta<\frac{1}{2}-\frac{\alpha}{4}$. □

Remark: Here the results in [10] and [7] are for the cases when $p-q$ and $2p-q$ is small. These results are special cases of Theorem 1, for $a=b=1$ and $a=2, b=1$, respectively.

Let us briefly summarize the above theorem by the following algorithm.

Algorithm 1

1: Input: RSA public key (e, N).
2: Output: The secret exponent d.
3: Step 1: Choose two coprime integers a and b which are less than $logN$. (The integers a and b can be generated by Stern-brocot tree.)
4: Step 2: Compute the convergent of $\frac{e}{N-\frac{a+b}{\sqrt{ab}}\sqrt{N}+1}$.
5: Step 3: For each convergent $\frac{m_i}{n_i}$, solve the equation $x^2-(N+1-\frac{em_i-1}{n_i})x+N=0$. If its roots are positive integers less than N, then return the secret exponents m_i.
6: Step 4: Return(failure).

Recall that in Blomer's theory [1] (Theorem 2), N can be factored in polynomial time if $\forall\ N$, e satisfying $ex+y=0mod\phi(N)$, with $x\leq\frac{1}{3}N^{\frac{1}{4}}$ and $|y|\leq cN^{-\frac{3}{2}}ex$, $c\leq 1$ and $p-q\geq cN^{\frac{1}{2}}$. Here from the above condition imply that $ex+y\neq 0$, therefore excluding the trivial congruences: since $c\leq 1$, we see that $|y|<ex$. This implies that $m>0$. Thus we consider $ex+y=m\phi(N)=m(pq-p-q+1)=m(N-p-q+1)$. This implies that $\frac{e}{N}-\frac{m}{x}=-\frac{m(p+q-1)+y}{Nx}$. If $|\frac{e}{N}-\frac{m}{x}|=|\frac{m(p+q-1)+y}{Nx}|<\frac{1}{2x^2}$, then the fraction $\frac{m}{x}$ is one of the convergent of $\frac{e}{N}$. Thus one need to find out the conditions such that $|m(p+q-1)+y|<\frac{N}{2x}$ is satisfied. Here notice that, instead of trying to find $\frac{m}{x}$ among the convergent of $\frac{e}{N}$, a better attempt will be to find $\frac{m}{x}$ among the convergent of $\frac{e}{\phi'(N)}$, where $\phi'(N)$ is a better estimate than N for $\phi(N)$. Following the idea of [10], $\phi'(N)$ has been taken as $N-\lfloor 2\sqrt{N}\rfloor$ and the continued fraction expression of $\frac{e}{N-\lfloor 2\sqrt{N}\rfloor}$ has been considered to estimate $\frac{m}{x}$ in [1] (Section 4). It has been proved in [1] (Theorem 4, Section 4) that p, q can be found in polynomial time for every N, e satisfying $ex+y=0mod\phi(N)$, with $x\leq\frac{1}{3}\sqrt{\frac{\phi(N}{e}}\ \frac{N^{\frac{3}{4}}}{p-q}$ and $|y|\leq\frac{p-q}{\phi(N)N^{\frac{1}{4}}}ex$. In [7], it has been shown that the class of weak keys identified in [1] (Theorem 2) can be extended by more than five times. Now, here arise a question: can we further extend the range of weak key? In this article we try to answer affirmatively. Using the method discussed in the above Theorem 1 for $a=3$ and $b=2$, we extend the range of weak key by more than 8 times than the range given in [1] and around 1.5 times than the range given in [7]. Now we start with the following lemma.

Lemma 1. *Let $ex+y=m\phi(N)$ for $m>0$. Then $|\frac{e}{N-\frac{5}{\sqrt{6}}\sqrt{N}+1}-\frac{m}{x}|<\frac{1}{2x^2}$ for $x\leq\frac{57}{20}N^{\frac{1}{4}}$ when $|y|\leq cN^{-\frac{3}{4}}ex$, where $c\leq 1$ and $p-q\geq cN^{\frac{1}{2}}$.*

Proof. The proof follows from the following steps:

Step 1. Since $N-\frac{5}{\sqrt{6}}\sqrt{N}+1<\phi(N)<N-2\sqrt{N}+1$, using [7] (Proposition 1). From

$$\begin{aligned}
N-\frac{5}{\sqrt{6}}\sqrt{N}+1 \ &< \ \phi(N)\\
\Rightarrow (p+q) \ &< \ \frac{5}{\sqrt{6}}\sqrt{N}. \qquad (2)
\end{aligned}$$

Similarly, from

$$\begin{aligned}
\phi(N) \ &< \ N-2\sqrt{N}+1\\
\Rightarrow 2\sqrt{N} \ &< \ p+q. \qquad (3)
\end{aligned}$$

Hence from Equations (2)and (3):

$$\begin{aligned}
(2-\frac{5}{\sqrt{6}})\sqrt{N} \ &< \ p+q-\frac{5}{\sqrt{6}}\sqrt{N}<0\\
\Rightarrow |(2-\frac{5}{\sqrt{6}}\sqrt{N}| \ &> \ |p+q-\frac{5}{\sqrt{6}}\sqrt{N}|\\
\Rightarrow (\frac{5}{\sqrt{6}}-2)\sqrt{N} \ &> \ |p+q-\frac{5}{\sqrt{6}}\sqrt{N}|.
\end{aligned}$$

Step 2. Since $|y|\leq cN^{-\frac{3}{4}}ex$, we have $|y|<xN^{\frac{1}{4}}$ as $e<N$ and $c\leq 1$.

Step 3. We know from [1], $\frac{3}{4}\frac{ex}{\phi(N)} \leq m \leq \frac{5}{4}\frac{ex}{\phi(N)}$. Now,

$$\begin{aligned}
&\frac{e}{N-\frac{5}{\sqrt{6}}\sqrt{N}+1} - \frac{m}{x} \\
= &\frac{ex - m(N+1-\frac{5}{\sqrt{6}}\sqrt{N})}{x(N+1-\frac{5}{\sqrt{6}}\sqrt{N})} \\
= &\frac{m\phi(N) - y - m(N+1-\frac{5}{\sqrt{6}}\sqrt{N})}{x(N+1-\frac{5}{\sqrt{6}}\sqrt{N})} \\
= &\frac{m(N+1-(p+q)) - y - mN - m + m\frac{5}{\sqrt{6}}\sqrt{N}}{x(N+1-\frac{5}{\sqrt{6}}\sqrt{N})} \\
= &\frac{m(-p-q+\frac{5}{\sqrt{6}}\sqrt{N}) - y}{x(N+1-\frac{5}{\sqrt{6}}\sqrt{N})}
\end{aligned}$$

By Step 1:

$$|\frac{e}{N-\frac{5}{\sqrt{6}}\sqrt{N}+1} - \frac{m}{x}| < \frac{m(\frac{5}{\sqrt{6}}-2)\sqrt{N}+|y|}{x(N-\frac{5}{\sqrt{6}}\sqrt{N})+1}.$$

Now,

$$\frac{m(\frac{5}{\sqrt{6}}-2)\sqrt{N}+|y|}{x(N-\frac{5}{\sqrt{6}}\sqrt{N}+1)} < \frac{1}{2x^2},$$

if $\frac{\frac{5}{4}\frac{ex}{\phi(N)}(\frac{5}{\sqrt{6}}-2)\sqrt{N}+xN^{\frac{1}{4}}}{x(N-\frac{5}{\sqrt{6}}\sqrt{N}+1)} < \frac{1}{2x^2}$, using Steps 2 and 3. That is, if $\frac{\frac{5}{4}(\frac{5}{\sqrt{6}}-2)\sqrt{N}+N^{\frac{1}{4}}}{(N-\frac{5}{\sqrt{6}}\sqrt{N}+1)} < \frac{1}{2x^2}$ (since $e < \phi(N)$, $\frac{e}{\phi(N)} < 1$), if $\frac{\frac{5}{4}\times 0.05\sqrt{N}}{N-\frac{5}{\sqrt{6}}\sqrt{N}+1} < \frac{1}{2x^2}$ (since $\frac{5}{\sqrt{6}} - 2 < 0.05$ and $\frac{5}{4}(\frac{5}{\sqrt{6}}-2)\sqrt{N}+N^{\frac{1}{4}} < \frac{5}{4}\times 0.05\sqrt{N}$, for large N.), if $\frac{5}{2}\times 0.05x^2 < N^{\frac{1}{2}} + \frac{1}{N^{\frac{1}{2}}} - \frac{5}{\sqrt{6}}$, if $x^2 < 8N^{\frac{1}{2}}$ (for large N), $x \leq 2\sqrt{2}N^{\frac{1}{4}}$, this implies that $x \leq 2(1.414)N^{\frac{1}{4}} \leq 2.828N^{\frac{1}{4}} \leq 2.85N^{\frac{1}{4}}$.

This shows that the class of weak keys identified in [1] (Theorem 2: $x \leq \frac{1}{3}N^{\frac{1}{4}}$) and [7] (Lemma 2, Section 3: $x \leq \frac{7}{4}N^{\frac{1}{4}}$) can be extended by $\frac{57\times 3}{20\times 1} = \frac{161}{20}$ and $\frac{57\times 4}{20\times 7} = \frac{57}{35}$ respectively, i.e, by more than 8 and 1.5 times. This also shows that Lemma [1] presents the class of new weak keys over [1] (Theorem 4, Section 4), when $\frac{e}{\phi(N)} > (\frac{20}{161c})^2$ for $\frac{20}{161} < c < \frac{1}{\sqrt{2}}$. □

Theorem 3. *Let $|ap-bq| \leq \frac{1}{2}N^{\alpha}$ where $0 < \alpha \leq 1$. Suppose e satisfies an equation $ex+y = m\phi(N)$, for $m > 0$. Then N can be factored in O(poly(log(N))) time when $0 < x \leq \frac{1}{6}\sqrt{\frac{\phi(N)}{e}}N^{\frac{1}{2}-\frac{\alpha}{4}}$ and $|y| \leq \frac{|ap-bq|}{\phi(N)N^{1/4}}ex$.*

Proof. Since $ex+y = m\phi(N)$, this implies that $m = \frac{ex+y}{\phi(N)}$. Using the bound on $|y|$, we have $m \leq \frac{ex}{\phi(N)}(1+\frac{|ap-bq|}{\phi(N)N^{\frac{1}{4}}})$. So

$$\begin{aligned}
&|\frac{e}{N-(\frac{a+b}{\sqrt{ab}})\sqrt{N}+1} - \frac{m}{x}| \\
= &\frac{|ex - m(N-\frac{a+b}{\sqrt{ab}}\sqrt{N}+1)|}{x(N-\frac{a+b}{\sqrt{ab}}\sqrt{N}+1)} \\
= &\frac{|m(\frac{a+b}{\sqrt{ab}}\sqrt{N}-p-q)|+|y|}{x(N-\frac{a+b}{\sqrt{ab}}\sqrt{N}+1)} \quad (\text{since } ex+y = m\phi(N)) \\
\leq &\frac{(\frac{ex}{\phi(N)}(1+\frac{|ap-bq|}{\phi(N)N^{\frac{1}{4}}}))(\frac{a+b}{\sqrt{ab}}\sqrt{N}-p-q)+\frac{|ap-bq|}{\phi(N)N^{\frac{1}{4}}}ex}{x(N-\frac{a+b}{\sqrt{ab}}\sqrt{N}+1)} \\
&(\text{using the upper bound of } m \ \&\ y) \\
= &\frac{(\frac{e}{\phi(N)}(1+\frac{|ap-bq|}{\phi(N)N^{\frac{1}{4}}}))(\frac{a+b}{\sqrt{ab}}\sqrt{N}-p-q)+\frac{|ap-bq|}{\phi(N)N^{\frac{1}{4}}}e}{(N-\frac{a+b}{\sqrt{ab}}\sqrt{N}+1)} \\
< &\frac{e}{\phi(N)}\frac{2N^{\frac{\alpha}{2}}+2N^{\frac{2\alpha}{2}-\frac{5}{4}}+N^{\frac{1}{2}-\frac{\alpha}{4}}}{N-\frac{a+b}{\sqrt{ab}}\sqrt{N}+1} \\
&(\text{using } |ap-bq| \leq N^{\frac{\alpha}{2}} \text{ and } |\tfrac{a+b}{\sqrt{ab}}\sqrt{N}-p-q| < 2N^{\frac{\alpha}{2}}) \\
< &\frac{e}{\phi(N)}\frac{3N^{\frac{\alpha}{2}}}{N-\frac{a+b}{\sqrt{ab}}\sqrt{N}+1} \\
< &\frac{e}{\phi(N)}18N^{\frac{\alpha}{2}-1} \quad (\text{assuming } N-\tfrac{a+b}{\sqrt{ab}}\sqrt{N}+1 > \tfrac{N}{6}).
\end{aligned}$$

Hence, we get $\frac{m}{x}$ via continued fraction expression of $\frac{e}{N-\frac{a+b}{\sqrt{ab}}\sqrt{N}+1}$, if $\frac{e}{\phi(N)}18N^{\frac{\alpha}{2}-1} < \frac{1}{2x^2}$, that is $x < \frac{1}{6}\sqrt{\frac{\phi(N)}{e}}N^{\frac{1}{2}-\frac{\alpha}{4}}$. Now, we have to show that the correct m and x yield the factorization of N. Since $ex+y = m(N-(p+q)+1)$, this implies that $N+1-\frac{ex}{m} = p+q+\frac{y}{m}$ since every parameter on the L.H.S. is now known to us, we can compute an approximation of $p+q$, up to some unknown error term $\frac{y}{m}$. Since $\frac{y}{m} \leq cN^{\frac{1}{4}}$, where c is independent of a, b. Hence, using the technique's of [1], we can easily factor N in polynomial time. □

Note 1. The result of [1] (Theorem 4, Section 4) states that N can be factorized in polynomial time if e satisfies the relation $ex + y = 0 \bmod \phi(N)$, with $0 < x \leq \frac{1}{3}\sqrt{\frac{\phi(N)}{e}}\frac{N^{\frac{3}{4}}}{\phi(N)N^{\frac{1}{4}}}$ and $|y| \leq \frac{p-q}{\phi(N)N^{\frac{1}{4}}}ex$. In our result $p-q$ is replaced by $ap-bq$ where a is coprime to b and $a \geq 1$. Thus the results of this section present new weak keys other than those presented in [1]. The result of [1] works efficiently when $p-q$ is upper bounded and our works gives better results when $|ap-bq|$ is upper bounded.

Note 2. Our result is also better than [7]. Since the result of [7] (Theorem 4, Section 3) works efficiently when $|\rho q-p|$ is upper bounded and our works gives better results when $|ap-bq|$ is upper bounded. Now we estimate the number of weak keys, the method is same as in [1]. First we use the existing result, i.e, lower bound theory which is as follows.

Lemma 2. *[1] (Lemma 6.) Let $f(N,e), g(N,e)$ be functions such that $f^2(N,e)g(N,e) < \phi(N,e)$, $f(N,e) \geq 2$ and $g(N,e) \leq f(N,e)$. The number of public keys $e \in Z^*_{\phi(N)}$, $e \geq \frac{\phi(N)}{4}$ that satisfy an equation $ex + y = 0 \bmod \phi(N)$ for $x \leq f(N,e)$ and $|y| \leq g(N,e)x$ is at least $\frac{f(N,e)g(N,e)}{8\log\log^2(N^2)} - O(f^2(N,e)N^\epsilon)$, where $\epsilon > 0$ is arbitrarily small for N suitably large. Hence, before presenting our estimate using similar analysis in [1], we define the class of weak keys as presented in [1].*

Definition 1. *Let C be a class of RSA public keys N, e. The size of the class C is defined by*

$$size_C(N) = |\{e \epsilon Z^*_{\phi(N)} | (N,e) \epsilon C\}|.$$

C is called weak if:

1) *$size_C(N) = \Omega(N^\gamma)$ for $\gamma > 0$.*
2) *There exists a probabilistic algorithm A that on every input $(N,e) \epsilon C$ outputs the factorization of N in time polynomial in $\log(N)$.*

The elements of a weak class are called weak keys.

Theorem 4. *Let $|ap - bq| = N^{\frac{1}{4}} + \gamma$ with $0 < \gamma \leq \frac{1}{4}$, further, let C be weak class that is given by the public key tuples N, e defined in Theorem 1 with the additional restrictions that $e \epsilon Z^*_{\phi(N)}$ and $e \geq \frac{\phi(N)}{4}$. Then $size_C(N) = \Omega(N^{\frac{3}{4}})$.*

Proof. Here $f(N,e) = \frac{1}{6}\sqrt{\frac{\phi(N)}{e}} N^{\frac{1}{2}-\frac{\alpha}{4}}$, $g(N,e) = \frac{|ap-bq|}{\phi(N)N^{1/4}} e$. It can be easily checked that these settings fulfill the requirements of Lemma 2:

$$\begin{aligned} f^2(N,e)g(N,e) &< \phi(N), \\ f(N,e) &\geq 2, \text{ and} \\ g(N,e) &\leq f(N,e). \end{aligned}$$

Hence we can apply Lemma 2. Since $g(N,e) = \Omega(N^\gamma)$, the term $\frac{f^2(N,e)g(N,e)}{8\log\log^2(N^2)}$ dominates the error term $O(f^2(N,e)N^\epsilon)$. Using $f^2(N,e)g(N,e) = \Omega(N^{\frac{3}{4}})$, we get the estimate. □

4 Conclusion.

In this paper we generalize the idea of Weger [10] for $a = b = 1$ and [7] for$a = 2, b = 1$, where a and b be small integers.We provide new weak keys over the work of Blomer & May [1] and Maitra & Sarkar[7] and to the best of our knowledge the range of weak keys identified in our paper have not been presented earlier. In *Lemma I* we used the value of $a = 3$, $b = 2$ from the idea given in *Theorem* 1 to set $N - \frac{5}{\sqrt{6}}\sqrt{N} + 1$ as a better estimate of $\phi(N)$.Here one question can be arisen (has been mentioned many times in the past research), whether exists a better method to evaluate the estimated value of $\phi(N)$? If any how we find the better estimate of $\phi(N)$ the boundary of the Wiener attack can be raised again as the accuracy of the estimate of $\phi(N)$. Using the notion of weak keys, as defined by [1], the results of this paper show that this set of RSA public keys is a class of new weak keys.

References

[1] J. Blomer and Alexander May, "A generalised Wiener attack on RSA", *PKC 2004*, LNCS 2947, pp. 1–13, 2004.

[2] D. Boneh and G. Durfee, "Cryptanalysis RSA with private key $d < N^{0.292}$", *Eurocrypt 1999*, LNCS 1592, pp. 1–11, 1999.

[3] D. Coppersmith, "Small solutions to polynomial equations and low exponent vulnerabilities", *Journal of Cryptology*, vol. 20, no. 1, pp. 39–50, 2007.

[4] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics - A Foundation for Computer Science, 2nd edition*, Addition-Wesley, 1994.

[5] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, London, 1965.

[6] H. W. Lenstra, "Factoring integers with elliptic curves", *Annals of Mathematics*, vol. 126, pp. 649–673, 1987.

[7] S. Maitra and S. Sarkar, "Revisiting Wiener's attack - New weak keys in RSA", *Lecture Notes in Computer Science*, LNCS 5222, pp. 228–243, 2008.

[8] R. L. Rivest, A. Shamir, and L. M. Adleman, "A method of obtaining digital signatures and public key cryptosystem", *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[9] L. Szöllösi, T. Marosits, and G. Feher, "Accelerating RSA encryption using random precalculations", *International Journal of Network Security*, vol. 10, no. 2, pp. 157–160, 2010.

[10] B. de Weger, "Cryptanalysis of RSA with small prime difference", *Proceedings of the conference on Applicable Algebra in Engineering, Communication and Computing (AAECC'02)*, pp. 17–28, 2002.

[11] M. J. Wiener, "Cryptanalysis of short RSA secret exponents", *IEEE Transactions on Information Theory*, vol. IT(36), pp. 553–558, 1990.

[12] S. M. Yen, S. Kim, S. Lim, and S. Moon, "Speed up with residue number system immune against hardware fault cryptanalysis", *Proceedings of the 4th International Conference on Information Security and Cryptology*, Lecture Notes in Computer Science, LNCS 2288, pp. 397-413, 2001.

Sahadeo Padhye received his B.Sc.and M.Sc. degree in Mathematics form Pt. Ravishankar Shukla University, Raipur. Chhattisgarh, India in 1999 and 2001. Council of Scientific and Industrial Research (CSIR), India has granted him Junior Research Fellowship (2002-2004). He did his Ph.D. form Pt. Ravishankar Shukla University, Raipur, India. He is a life member of Cryptology Research Society of India (CRSI) and a member of

International Association of Cryptologic Research (IACR). His area of interest is Public Key Cryptography based on elliptic curve and ID-Based digital signature. Presently he is working as Assistant Professor in Motilal Nehru National Institute of Technology, Allabahad, India.

Navaneet Ojha received his B.Sc. and M.Sc. degree from Purvanchal University, Jaunpur, Utter Pradesh, India in the year 2001 and 2004 respectively. He is a life member of Cryptology Research Society of India (CRSI). His area of interest is Public Key Cryptosystem based on Factoring Problem. Presently he is pursuing his Ph.D. degree in Motilal Nehru National Institute of Technology, Allabahad, India.