Extension of de Weger's Attack on RSA with Large Public Keys

Nicolas T. Courtois, Theodosis Mourouzis and Pho V. Le
Department of Computer Science, University College London, Gower Street, London, U.K.

Keywords: RSA, Cryptanalysis, Weak Keys, Exponent Blinding, Wiener's Attack, de Weger's Attack, Large Public Keys.

Abstract: RSA cryptosystem (Rivest et al., 1978) is the most widely deployed public-key cryptosystem for both encryption and digital signatures. Since its invention, lots of cryptanalytic efforts have been made which helped us to improve it, especially in the area of key selection. The security of RSA relies on the computational hardness of factoring large integers and most of the attacks exploit bad choice parameters or flaws in implementations. Two very important cryptanalytic efforts in this area have been made by Wiener (Wiener, 1990) and de Weger (Weger, 2002) who developed attacks based on small secret keys (Hinek, 2010).The main idea of Wiener's attack is to approximate the fraction $\frac{e}{\varphi(N)}$ by $\frac{e}{N}$ for large values of N and then make use of the continued fraction algorithm to recover the secret key d by computing the convergents of the fraction $\frac{e}{N}$. He proved that the secret key d can be efficiently recovered if $d < \frac{1}{3}N^{\frac{1}{4}}$ and $e < \varphi(N)$ and then de Weger extended this attack from $d < \frac{1}{3}N^{\frac{1}{4}}$ to $d < N^{\frac{3}{4}-\beta}$, for any $\frac{1}{4} < \beta < \frac{1}{2}$ such that $|p-q| < N^{\beta}$. The aim of this paper is to investigate for which values of the variables σ and $\Delta = |p-q|$, RSA which uses public keys of the special structure $E = e + \sigma\varphi(N)$, where $e < \varphi(N)$, is insecure against cryptanalysis. Adding multiples of $\varphi(N)$ either to e or to d is called Exponent Blinding and it is widely used especially in case of encryption schemes or digital signatures implemented in portable devices such as smart cards (Schindler and Itoh, 2011). We show that an extension of de Weger's attack from public keys $e < \varphi(N)$ to $E > \varphi(N)$ is possible if the security parameter σ satisfies $\sigma \leq N^{\frac{1}{2}}$.

1 INTRODUCTION

The RSA cryptosystem was invented by Rivest, Shamir and Adleman in 1978 (Rivest et al., 1978) and is considered among the most practical and popular asymmetric key cryptosystem in the cryptographic community. It is widely used in many applications such as access control, electronic voting and online banking (Schneier, 1996).

The security of RSA cryptosystem is based entirely on the structure of the multiplicative group $\mathbb{Z}/N\mathbb{Z}$, where N is the product of two large primes p and q, typically of equal bit length. Thus, N is selected in such a way such that the problem of factoring the modulus N is computationally hard. It can be proved that factoring N is polynomially (in time) equivalent to the problem of computing the secret key d if $d < N$ and it is an open problem to prove or disprove the polynomial time equivalence of these problems to the problem of extracting e^{th}-roots in the ring $\mathbb{Z}_{\mathbb{N}}$ (Goldreich, 2008). However, most of the attacks are based on misuse of the system, bad choice parameters or flaws in implementations (Joux, 2009). The significance of cryptographic key size to the security of cryptosystem is emphasized by (Lenstra and Verheul, 2000), where they offer guidelines for the determination of key sizes for symmetric cryptosystems, RSA and discrete logarithm based cryptosystems over finite fields and groups of elliptic curves over prime fields.

RSA algorithm is defined by the following four algorithms:

1. **Modulus-generation:** Given the security parameter of size n, generate two distinct large primes p, q with $q < p < 2q$. Then the modulus is $N = pq$.
2. **Key-generation:** $(e,d) \leftarrow KeyGen(p,q)$

   Given p and q, compute $\varphi(N) = (p-1)(q-1)$.Then pick $e \in \mathbb{Z}^*_{\varphi(N)}$ (i.e $(e,\varphi(N)) = 1$) and let d be its multiplicative inverse ($ed \equiv 1 \bmod \varphi(N)$)
3. **Encryption:** M is encrypted via the power map $x \to x^e$ to give $C \equiv M^e \bmod (N)$
4. **Decryption:** C is decrypted via the power map $x \to x^d$: $C^d \equiv (M^e)^d \equiv M \bmod (N)$

T. Courtois N., Mourouzis T. and V. Le P..
Extension of de Weger's Attack on RSA with Large Public Keys.
DOI: 10.5220/0004054201450153
In *Proceedings of the International Conference on Security and Cryptography* (SECRYPT-2012), pages 145-153
ISBN: 978-989-8565-24-2

RSA is an efficient system for the following reasons (Joux, 2009):

1. Modulus N can be constructed efficiently since we have the ability to pick large primes at random, thanks to the efficient primality testing algorithms (Crandall and Pomerance, 2005).
2. Encryption and Decryption permutations can be efficiently computed given N and e (or d). This can be very efficient by using fast modular exponentiation algorithms.
3. Computations of the decryption exponents is achieved easily using Euclid's algorithm

Most of the existing attacks on the RSA cryptosystem are factorization algorithms. Since factoring an RSA modulus of the form $N = pq$ is assumed to be a hard computational problem, the aim of a cryptanalyst is to identify practically interesting cases where the underlying factorization problem is solvable in polynomial time. A plethora of attacks recover weak keys from the information revealed by the public exponent e (Hinek, 2010). Wiener (Wiener, 1990) was the first to prove that the RSA modulus N can be factored for every public exponent $e < \varphi(N)$ with small secret keys d satisfying $d < \frac{1}{3}N^{\frac{1}{4}}$. de Weger (Weger, 2002) extended this bound from $d < \frac{1}{3}N^{\frac{1}{4}}$ to $d < N^{\frac{3}{4}-\beta}$, for any $\frac{1}{4} < \beta < \frac{1}{2}$ such that $|p-q| < N^{\beta}$. However, all existing attacks related to small secret keys that are found in the literature consider only cases where $e < \varphi(N)$.

Our Contribution: In this paper we examine the security of RSA which uses large public keys of the form $E = e + \sigma\varphi(N)$, where $e < \varphi(N)$, $\sigma \leq N^{\frac{1}{2}}$ and $\Delta = |p-q| < N^{\beta}$ for any $\beta \in [\frac{1}{4}, \frac{1}{2}]$. These keys of special structure are proposed by Wiener as countermeasures against his own attack. Today, this method of generating public keys e is employed by the industry and is called exponent blinding. Exponent blinding is considered as a countermeasure against Differential Power Analysis (DPA) (Schindler and Itoh, 2011). However, cryptanalysis of RSA which uses public keys of this structure is less widely studied.

We perform a security analysis of how successful the attack is on RSA cryptosystem for different values of the variable σ and different values of the prime difference $|p-q|$. We implement our attack which is an extension of de Weger's attack using Victor Shoup's Number Theory Library (NTL) (Shoup, 2009). Our implementations suggest that the size of σ is one of the main factors that determines the security and the efficiency of the system and we prove that our attack is successful if $\sigma \leq N^{\frac{1}{2}}$.

2 BACKGROUND MATHEMATICS

In this section we briefly discuss the *Continued Fraction* algorithm which is another variant of the Euclidean Division algorithm. We also state Legendre's rational approximation theorem which is what inspired Wiener to develop his attack.

Continued Fraction:
The *continued fraction expansion* of a rational number α is (Hardy and Wright, 2008) :

$$\alpha = \frac{p_n}{q_n} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ldots + \cfrac{1}{a_n}}}} \tag{1}$$

where $a_0 \in \mathbb{Z}$ and $a_i \in \mathbb{N}$ for $i \geq 0$.

The numbers $a_0, a_1, a_2, \ldots, a_n$ are called the *partial quotients*. In short, we denote the continued fraction expansion of a rational number α as $[a_0, a_1, \ldots, a_n]$ and for $i \geq 0$ the rationals $\frac{p_i}{q_i} = [a_0, a_1, \ldots, a_i]$ are called the *convergents* of the continued fraction expansion of α. If $\alpha \in \mathbb{Q}$ then the continued fraction expansion is finite and the continued fraction algorithm finds the convergent in time $O((\log(\frac{1}{\alpha}))^2)$.

The convergents of the continued fraction expansion can be computed recursively as stated by the following lemma.

Lemma 1. *The convergents* $\frac{p_n}{q_n}$ *can be computed using the following recursive relations:*

1. $p_0 = a_0,\ q_0 = 1$ (2)
2. $p_1 = a_0 a_1 + 1,\ q_1 = a_1$ (3)
3. $p_n = a_n p_{n-1} + p_{n-2}$,
   $q_n = a_n q_{n-1} + q_{n-2}$ for $n \geq 2$ (4)

Proof: Proof can be found in standard number theory textbooks (Hardy and Wright, 2008). $\square$

We end this introductory part by stating the famous Legendre's Approximation Theorem. This theorem is very important in cryptanalysis since it allows us to find a good rational approximation of any irrational number in polynomial time. Polynomial-time algorithms make implementations of theoretical attacks against cryptosystems feasible in practice.

Theorem 2. ***[Legendre's Theorem in Diophantine Approximations].*** *Let* $\alpha \in \mathbb{Q}$.
If $|\alpha - \frac{p}{q}| < \frac{1}{2q^2}$ *for some* $p, q \in \mathbb{Z}$*, then* $\frac{p}{q}$ *is a convergent arises from the continued fraction expansion of* α.

Proof: Proof can be found in standard number theory textbooks (Hardy and Wright, 2008). □

3 CRYPTANALYSIS OF RSA

A very basic question that we deal up with in the rest of this paper is:

Question: *When does e provide enough information to factor N?*

At first sight, it is not obvious at all that the public key exponent e may leak out any useful information which allows an attacker to break the cryptosystem by solving the underlying integer factoring problem in polynomial time. Since modular exponentiation is slow, it is very tempting for the crypto-designers to use public exponents e of a very special structure to balance decryption efficiency and security. There is inherent danger if the public key exponent e is chosen such that the corresponding secret key d is small. For example, every tuple $(N = pq, e)$ with $e = kq$ for some $k \in \mathbb{Z}$ such that $1 < k < p$ provides no security at all, since $GCD(N, e) = q$.

In the rest of this section we make an introduction to the state of art regarding the existing attacks on RSA cryptosystem using the notion of weak keys (May, 2003). Let us first formalize the notion of weak keys in the following way.

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

$size_C(N) := |\{e \in Z^*_{\varphi(N)} | (N, e) \in C\}|$. C is called weak if:

1. $size_C(N) = O(N^\gamma)$ for some $\gamma > 0$

2. There exists a probabilistic algorithm A that on every input $(N, e) \in C$ outputs the factorization of N in polynomial time in $\log N$.

The elements of a weak class are called weak keys.

We postpone details on Wiener's and de Weger's attacks until the next section, and summarize other types of attacks here. First, Fermat (McKee, 1999) shows that when the distance between the two primes $\Delta = |p - q| < cN^{1/4}$ for some constant c, then N can be factored efficiently. One may factor N by testing all cases for:
$x = \lceil 2N^{1/2} \rceil, x = \lceil 2N^{1/2} \rceil + 1, \ldots,$ until $x^2 - 4N$ is a square.
A solution can be found efficiently whenever $\Delta < cN^{1/4}$ since the number of trials is approximately $x - 2N^{1/2} = p + q - 2N^{1/2} < \frac{\Delta^2}{4N^{1/2}}$.

Thus if $|p - q| < cN^{1/4}$ holds, the number of trials is at most $\dfrac{c^2}{4}$ for some constant c.

Dujella (Dujell and Ibrahimpasic, 2008) proposed a new variant of Wiener's attack, which combines the results on Diophantine approximations of the form $|\alpha - \frac{p}{q}| < \frac{c}{q^2}$, and meet in the middle variant for testing the candidates of the form $rq_{m+1} + sq_m$ for the secret key. This new variant improves the range of weak keys by a factor of 2^{30} and improves the complexity of the attack by a constant.

Notable improvements are made by Boneh and Durfee (Boneh and Durfee, 2000) who heuristically but practically used the LLL algorithm for finding short vectors in lattices to show that RSA is insecure whenever $d < N^{1-\frac{1}{\sqrt{2}}}$. However, they conjecture that RSA is insecure if $d < N^{1/2}$ apart from an espilon.

Lastly, Alexander May (May, 2003) proved that RSA modulus N can be successfully factored not only when d is small but even when it has small decomposition. He proved that N can be factored in polynomial time whenever $d < -\frac{w}{z} mod \varphi(N)$ with $w \leq \frac{N^{1/4}}{3}$ and $|z| = O(N^{-3/4}ew)$.

In this paper we study the weaknesses of RSA when public keys of the form $E = e + \sigma\varphi(N)$ are used, for $e < \varphi(N)$ and σ an input parameter. We apply the continued fraction algorithm on RSA cryptosystem which uses these special keys to recover the secret key. Adding multiples of $\varphi(N)$ either to e or to d is called Exponent Blinding and it is widely used especially in case of encryption schemes or digital signatures implemented in portable devices such as smart cards (Schindler and Itoh, 2011).

3.1 A Detailed Analysis of Wiener's Attack

Wiener was the first who observed that information encoded in the public exponent e can reveal the factors of the modulus N. He showed that every public key which corresponds to a secret key such that $d < \frac{1}{3}N^{\frac{1}{4}}$ yields the factorization of N in polynomial time in the bit-size of N.

Below we state and prove his attack.

Theorem 3. ***[Wiener].*** *Suppose p, q are primes with $q < p < 2q$. Let $N = pq$ and let $d \geq 1$, $e < \varphi(N)$ such that $ed \equiv 1 \bmod \varphi(N)$. If $d < \frac{1}{3}N^{\frac{1}{4}}$, then d can be recovered in polynomial time in* $\log N$.

Proof: Since $ed \equiv 1 \bmod \varphi(N)$, there is a k such that $ed = 1 + k\varphi(N)$ *(5)*. Rewrite this as

$$\left| \frac{e}{\varphi(N)} - \frac{k}{d} \right| = \frac{1}{d\varphi(N)} \tag{6}$$

When N is large, $\varphi(N) \simeq N$, which implies $\frac{e}{N} \simeq \frac{k}{d}$. Since p,q are of the same bit-size, $N - \varphi(N) < 3\sqrt{N}$. Therefore,

$$\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{3k}{d\sqrt{N}} < \frac{1}{dN^{\frac{1}{4}}} < \frac{1}{2d^2} \tag{7}$$

Then according to Legendre's Approximation Theorem, $\frac{k}{d}$ equals to a convergent of the continued fraction expansion of $\frac{e}{N}$. Since the number of steps in the continued fraction expansion of $\frac{e}{N}$ is at most a constant times $\log N$, then using Attack Algorithm in section 3.3 with input (e,N)

$$d = d_i forsomei \in \{1,2,\ldots,\log N\}\square \tag{8}$$

Wiener's attack does not highlight any flaws in the design of the RSA cryptosystem but only shows that an attack can be implemented in polynomial time if the public-key and secret-key satisfy some bounds. His attack claims that RSA becomes vulnerable if the users use insecure keys. However, he proposed also some countermeasures against his attack which we mention below.

Countermeasures Against Wiener's Attack:

1. If $e > N^{3/2}$ then the continued fraction algorithm is not guaranteed to work for any size of the secret key d. *Lemma 4* proves this result.
2. Increasing $GCD(p-1,q-1)$, since the size of secret key d that can be found is inversely proportional to this value. However, this may lead to other problems.
3. Use unbalanced primes so that $p+q$ becomes larger, decreasing in this way the range of weak keys.

Lemma 4. *Wiener's attack based on continued fraction is completely ineffective when $e > N^{\frac{3}{2}}$.*

Proof: Consider the approximation $\frac{e}{N} \simeq \frac{k}{d}$. So, if $e > N^{\frac{3}{2}}$, then $k \simeq d\sqrt{N}$. Substituting k into the proof of Theorem 3, we have $3 < \frac{1}{2d^2}$. This contradicts the assumption that $d \geq 1$. $\square$

3.2 Extension of de Weger's Attack on RSA with Large Public Keys

In this section we investigate the ranges of σ and the *prime difference* $\Delta = |p-q|$ in which RSA is insecure even when large public keys of the form $E = e + \sigma\varphi(N)$ are used.

We implement our attack using Victor Shoup's Number Theory Library (NTL) (Shoup, 2009) and present results for different bit-values of the modulus N and for different values of $\Delta = |p-q| < N^{\beta}$. Our implementations suggest that the size of σ is one of the main factors that determines the security and efficiency of the system. Below we state and prove some *Lemmas* which help us to formalize our attack.

Lemma 5. *Suppose N is the product of two distinct primes p and q. If N and $\varphi(N)$ are known, then p,q can be trivially found.*

Proof: By definition,

$$\varphi(N) = (p-1)(q-1) = N + 1 - (p+q) \tag{9}$$

Thus, for some constant c as LHS is known,

$$p + q = N - \varphi(N) + 1 = c \tag{10}$$

Substituting q by $\frac{N}{p}$ we get a quadratic equation involving only p. Solving the equation we obtain p,q simultaneously.$\square$

Lemma 6. *If $N = pq$ and $\Delta = |p-q|$, then*

$$0 < p + q - 2\sqrt{N} < \frac{\Delta^2}{4\sqrt{N}} \tag{11}$$

Proof: Note $\Delta = |p-q|$. So,

$$\Delta^2 = |p-q|^2 = p^2 + q^2 - 2N \tag{12}$$

$$= (p+q)^2 - 4N \tag{13}$$

$$= (p + q - 2\sqrt{N})(p + q + 2\sqrt{N}) \tag{14}$$

$\square$

Lemma 7. ***[de Weger's Attack].*** *Suppose p,q are two primes such that $q < p < 2q$. Consider the RSA cryptosystem with $N = pq$, $d \geq 1$ and $e < \varphi(N)$ such that $ed \equiv 1 \ mod\ \varphi(N)$. If $\delta < \frac{3}{4} - \beta$, with $\beta \in [\frac{1}{4}, \frac{1}{2}]$ and if $d < N^{\delta}$, then d can be found efficiently.*

Proof: Proof can be found in (Weger, 2002).$\square$

The following *Lemma* claims an extension of de Weger's attack on RSA cryptosystem which makes use of large public keys E of the form $e + \sigma\varphi(N)$. We construct and implement our attack based on this result.

Lemma 8. *Suppose p and q are two primes such that $q < p < 2q$. Consider the RSA cryptosystem with $N = pq$, $d \geq 1$ and $E = e + \sigma\varphi(N)$ $(e < \varphi(N))$ such that $Ed \equiv 1 \ mod\ \varphi(N)$. If $\delta < \frac{3}{4} - \beta$, with $\beta \in [\frac{1}{4}, \frac{1}{2}]$ and if $d < \frac{N^{\delta}}{\sqrt{1+\sigma}}$, then d can be recovered in polynomial time in $\log N$.*

Proof: From $Ed \equiv 1 \bmod \varphi(N)$, there exists an integer K such that

$$Ed = 1 + K\varphi(N) \tag{15}$$

Since

$E = e + \sigma\varphi(N) < (1+\sigma)\varphi(N)$ and $\frac{1}{N-2\sqrt{N}+1} < \frac{1}{\varphi(N)}$, it implies

$$\left|\frac{E}{N-2\sqrt{N}+1} - \frac{K}{d}\right|$$

$$< E\left|\frac{1}{N-2\sqrt{N}+1} - \frac{1}{\varphi(N)}\right| + \left|\frac{E}{\varphi(N)} - \frac{K}{d}\right| \quad (16)$$

$$< (1+\sigma)\varphi(N)\frac{|(N-2\sqrt{N}+1)-\varphi(N)|}{(N-2\sqrt{N}+1)\varphi(N)} + \frac{1}{d\varphi(N)}$$

$$< \frac{1+\sigma}{\varphi(N)}(p+q-2\sqrt{N}) + \frac{1}{d\varphi(N)}$$

$$< \frac{1+\sigma}{\varphi(N)}\left(\frac{\Delta^2}{4\sqrt{N}} + \frac{1}{d}\right). \; (17)$$

For $N > 64$, $d < \sqrt{N} < \frac{N}{8}$. Thus we have $\varphi(N) > \frac{3}{4}N$ and $N > 8d$. Embedding the conditions $\Delta < N^{\beta}$ and $d < N^{\delta}$ on the inequality above yields,

$$\left|\frac{E}{N-2\sqrt{N}+1} - \frac{K}{d}\right| < \frac{1+\sigma}{3}N^{2\beta-\frac{3}{2}} + \frac{4(1+\sigma)}{3N^{1+\delta}} \quad (18)$$

$$< \frac{(1+\sigma)}{3}N^{2\beta-\frac{3}{2}} + \frac{1+\sigma}{6N^{2\delta}} \quad (19)$$

If $2\beta - \frac{3}{2} = -2\delta$ we get,

$$\left|\frac{E}{N-2\sqrt{N}+1} - \frac{K}{d}\right| < \frac{1+\sigma}{2N^{2\delta}} \quad (20)$$

Therefore, if $d < \frac{N^{\delta}}{\sqrt{1+\sigma}}$ then,

$$\left|\frac{E}{N-2\sqrt{N}+1} - \frac{K}{d}\right| < \frac{1}{2d^2} \quad (21)$$

By Legendre's Approximation Theorem, we can find the fraction $\frac{K}{d}$ using the convergents of the continued fraction expansion of $\frac{E}{N-2\sqrt{N}+1}$. Feeding $(E, N-2\sqrt{N}+1)$ as input, the Attack Algorithm in Section 3.3 will output the secret key d in polynomial time in $\log N$.$\square$

In the following *Lemma* we prove a theoretical bound for σ which is a threshold for our attack to work in polynomial time.

Lemma 9. ***[Bound for σ].*** *The extended de Weger's attack can find d if $d < \frac{N^{\delta}}{\sqrt{1+\sigma}}$ for any $\sigma \leq N^{\frac{1}{2}}$.*

Proof: We proved that for any public key of the form $E = e + \sigma\varphi(N)$, then the secret key d is recoverable if $d < \frac{N^{\delta}}{\sqrt{1+\sigma}}$. According to de Weger, the attack is considered as non trivial if $d < N^{\delta}$ where $\frac{1}{4} < \delta < \frac{1}{2}$. Suppose that $\sigma = N^{\alpha}$ for some constant α, then $d < \frac{N^{\delta}}{N^{\frac{\alpha}{2}}}$. For a non-trivial attack we need to have $\frac{1}{4} < \delta - \frac{\alpha}{2} < \frac{1}{2}$. Thus, $2\delta - 1 < \alpha < 2\delta - \frac{1}{2}$. Since $\frac{1}{4} < \delta < \frac{1}{2}$, we have that $\alpha \leq 2 \cdot max[\frac{1}{4}, \frac{1}{2}] - \frac{1}{2} = 2.\frac{1}{2} - \frac{1}{2} = \frac{1}{2}$. Clearly, the attack will succeed when $\alpha \leq \frac{1}{2}$.$\square$

3.3 Implementation of Attack and Results

We implemented our suggested attack using Victor Shoup's Number Theory Library and run the algorithm on a 1.67 GHz Intel Centrino Duo with Unix OS. The pseudocode of our implementation is presented as follows.

Attack Algorithm: $E = e + \sigma\varphi(N), d < \frac{N^{\delta}}{\sqrt{1+\sigma}}$

Input: $(E, N-2\sqrt{N}+1)$ and $i = 0$
Output: the prime factors p and q.

Step 1: Compute a_i
Step 2: Compute:

$$K_i = a_i p_{i-1} + p_{i-2} \; (22)$$
$$d_i = a_i q_{i-1} + q_{i-2} \; (23)$$

Step 3: **If** $d_i = 2u+1, u \in \mathbf{Z}^+$: Proceed to Step 4.
Else: Increase i by 1 and Go To Step 1.
Step 4: Compute $\varphi(N) = \frac{Ed_i - 1}{K_i}$. *(24)*
Step 5: Compute $b = N - \varphi(N) + 1 = (p+q)$. (25)
Step 6: **If** $b = 2u$: Proceed to Step 7.
Else: Increase i by 1 and Go To Step 1.
Step 7: Compute $r = b^2 - 4N$. *(26)*
Step 8: **If** $r < 0$: Increase i by 1 and Go To Step 1.
Else If $r > 0$: Compute:

$$p = \frac{b}{2} + \frac{\sqrt{r}}{2} \; (27)$$
$$q = \frac{b}{2} - \frac{\sqrt{r}}{2} \; (28)$$

Step 9: **If** $N = p \cdot q$, where $p > q > 1$:
Output p and q then $EXIT$
Else: Increase i by 1 and Go To Step 1.

At the first stage, we ran the algorithm for different values of N, β, σ on RSA cryptosystem which uses public keys of the form $E = e + \sigma\varphi(N)$ where the corresponding secret key satisfies the bound $d < \frac{N^{\delta}}{\sqrt{1+\sigma}}$. During our experiments, we generated $10,000$ pairs (p,q) of primes and then applied the extended de Weger's attack on the corresponding RSA cryptosystem. We consider a pair (p,q) as successful if de Weger's attack succeeds in recovering the secret key d and we set the probability of success for a given cryptosystem of modulus N of n-bits as the ratio of the number of successful pairs (p,q) divided by $10,000$. It can be seen from *Table* 1, that if $\sigma \leq N^{\frac{1}{2}}$ and the corresponding secret key d satisfies $d < \frac{N^{\delta}}{\sqrt{1+\sigma}}$ for any $\delta < \frac{3}{4} - \beta$ such that $|p-q| = N^{\beta}$, then the probability of success of our attack is 1. We tested modulus $N = 768, 1024$ bits, for $\sigma = N^{\frac{1}{8}}, N^{\frac{1}{4}}, N^{\frac{3}{8}}, N^{\frac{1}{2}}$ and $\beta = \frac{6}{16}, \frac{7}{16}$. In all cases we computed successfully the secret key d. Additionally, we tested the algorithm on RSA cryptosystem where the secret key d lies in the interval $\frac{N^{\delta}}{\sqrt{1+\sigma}} < d < N^{\delta}$ in order to examine how efficient is de Weger's attack beyond this bound. *Table* 2 shows that the probability of success is still large enough in this range. For example, given modulus N of 768 bits where $\sigma = 256$, $|p-q| < N^{\frac{6}{16}}$ and $d < N^{\frac{6}{16}}$ we succeed in recovering d in 3,395 pairs (p,q). This shows that even if the secret key is beyond our proved bound, de Weger's attack is still successful with considerable probability.

Table 1: $E = e + \sigma\varphi(N)$ with $e < \varphi(N)$. (100% success)

N (bits)	σ	Δ	$d < \frac{N^{\delta}}{\sqrt{1+\sigma}}$	**Factoring Time(s)**
768	$N^{\frac{1}{8}}$	$N^{\frac{6}{16}}$	$N^{\frac{5}{16}}$	1.89
768	$N^{\frac{1}{4}}$	$N^{\frac{6}{16}}$	$N^{\frac{4}{16}}$	1.45
768	$N^{\frac{3}{8}}$	$N^{\frac{6}{16}}$	$N^{\frac{3}{16}}$	1.16
768	$N^{\frac{1}{2}}$	$N^{\frac{6}{16}}$	$N^{\frac{2}{16}}$	0.61
1024	$N^{\frac{1}{8}}$	$N^{\frac{7}{16}}$	$N^{\frac{4}{16}}$	3.17
1024	$N^{\frac{1}{4}}$	$N^{\frac{7}{16}}$	$N^{\frac{3}{16}}$	2.26
1024	$N^{\frac{3}{8}}$	$N^{\frac{7}{16}}$	$N^{\frac{2}{16}}$	1.41
1024	$N^{\frac{1}{2}}$	$N^{\frac{7}{16}}$	$N^{\frac{1}{16}}$	0.68

Table 2: $E = e + \sigma\varphi(N)$ with $e < \varphi(N)$.

N (bits)	σ	Δ	$d < N^{\delta}$	**Success** (%)	**Time** (s)
768	$N^{\frac{1}{8}}$	$N^{\frac{6}{16}}$	$N^{\frac{5}{16}}$	33.95	89.55
768	$N^{\frac{1}{4}}$	$N^{\frac{6}{16}}$	$N^{\frac{4}{16}}$	27.18	91.32
768	$N^{\frac{3}{8}}$	$N^{\frac{6}{16}}$	$N^{\frac{3}{16}}$	21.26	95.91

Figure 1 illustrates how σ affects the success rate on a non-reduced weak keys range. As a non-reduced weak keys range we consider the interval $\frac{N^{\delta}}{\sqrt{1+\sigma}} <$

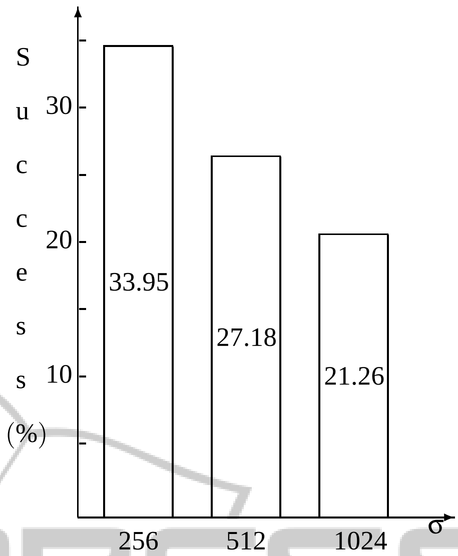

Figure 1: Figure 1: Success vs. σ ($\beta = \frac{6}{16}$).

$d < N^{\delta}$. As we see from the graph on a prime difference $|p-q| = N^{\frac{6}{16}}$ for $\sigma = 256, 512, 1024$ the average computational time (in seconds) taken to break RSA with probabilities 0.34, 0.27 and 0.21 respectively is 89.55s, 91.55s and 95.91s respectively. This does not suggest any strong relation between the average time taken to break RSA with a given probability of success and the value σ and this will be our future work to further examine.

We illustrate the efficiency of our attack with the following example:

Example 1: $E = e + \sigma\varphi(N)$**, with** $\sigma = N^{\frac{1}{8}}$**.**
Given the public key pair (E,N) as follows:

E = 4473293731721379708326616600641371492220
845230119444751885441402488136379218230 4
2580303555067640409493419404332664472448
0714478038456529674771687629881162322755
4678961978028136424180400714868424766444
8354895772013522056396609272682724216109
0330452630661776127401059497980897807338
6196848366948293603278560822708221179375
21087245892975144336823503 9

N = 1361103142776844843270777920580365159157
6601006345508838411887727879556293248064
2249596860481164422051701139230898415566
4424931166293389440803680740555437487284
6167304010906805090338353028590696012084
4307585718231100135485265240804855620064
1203400770888586653001891061900176260174
7649475896425686571068917532 1.

Invoke Attack Algorithm with (E,N) as input.

These are the first 160 *partial quotients* of $\dfrac{E}{N}$:
$[$328652075741682697961546789483959181844, 1, 27, 1, 1, 1, 1, 3, 1, 96, 9, 3, 1, 2, 1, 1, 2, 1, 4, 3, 1, 1, 4, 2, 1, 1, 1, 3, 1, 4, 3, 3, 1, 5, 5, 35, 93, 1, 2, 1, 50, 1, 6, 1, 18, 1, 4, 3, 1, 1, 8, 1, 2, 1, 1, 15, 1, 1, 17, 1, 10, 1, 8, 9, 2, 2, 3, 5, 1, 2, 1, 4, 1, 7, 5, 6, 1, 4, 2, 1, 8, 1, 2, 3, 1, 167, 2, 1, 2, 1, 1, 4, 83, 1, 39, 1, 4, 4, 1, 2, 3, 4, 1, 1, 3, 4, 1, 4, 3, 2, 2, 3, 1, 1, 1, 9, 10, 1, 1, 5, 1, 1, 1, 1, 11, 1, 2, 5, 3, 1, 5, 2, 1, 2, 6, 6, 1, 3, 1, 2, 2, 3, 1, 1, 10, 1, 14, 1, 1, 1, 3, 2, 1, 8, 6, 2, 1, 2, 32, 1, ...$]$.

The correct match for K, d are found to be:

K = 3070987483608851575982136048729894369853
4219871516636651327662263788394181486258
215892561331634184862899678187125943

d = 9344190133832039329908147240511603850575
5034440689899579037402947439951867059

This reveals the prime factors:

p = 1166663251661268725389428824859985517545
9908219624903472802403412154892075707775
6374879316119253701312036058191983768080
80007811078043670884807797534409911

q = 1166663251661268725336788995672885969781
2927977819680784988846996724342996653178
7411501168071305034508471832382745635149
76500711474673711625513687790363311.

The values δ and β are also calculated,
$\delta \approx 0.249796 < \dfrac{1}{4}$ and $\beta \approx 0.437217 < \dfrac{7}{16}$.
This shows that the range of weak keys has been slightly reduced.

The next example illustrates an instance where the secret key d can be found beyond the expected bound.

Example 2: $E = e + \sigma\varphi(N)$**, with** $\sigma = 1024$ Given the public key pair (E, N) as follows:

E = 8012376714025878357440941612240451226789
0791942096897899946588168355428594094184
5061181447285536558728607532595384614286
3319668080055405832203067073913077206415
1981240378734125396032476391897771717839
8820453182176280588447463505434327708387
9171785105345860294406474630477546282382
2809174314987563975138481387989

N = 7818698191737701140183794353099300460937
4874139988345505285292453980805767409916
8941897484632146251708594501064287176001
1783827092047583047572306308365275614833
5571512000452112721211954037224024252600
6261468265126625396332752868126228267183
5447353400369974141018700284783931591799
8566887250342874340484010853.

Invoke Attack Algorithm with (E, N) as input. These are the first 170 *partial quotients* of $\dfrac{E}{N}$:
$[$1024, 1, 3, 2, 1, 2, 3, 5, 1, 4, 1, 6, 1, 19, 1, 2, 1, 2, 2, 2, 5, 2, 16, 27, 1, 3, 11, 2, 1, 5, 3, 2, 1, 7, 2, 2, 1, 3, 1, 2, 3, 2, 2, 13, 213, 1, 21, 1, 3, 3, 10, 1, 9, 8, 4, 2, 1, 14, 2, 1, 33, 1, 1, 1, 7, 1, 42, 6, 1, 1, 326, 2, 3, 13, 6, 4, 4, 8, 1, 2, 5, 1, 2, 2, 2, 1, 1, 5, 4, 1, 3, 1, 2, 1, 14, 7, 57, 1, 1, 10, 2, 2, 3, 2, 58, 13, 2, 25, 2, 1, 8, 3, 1, 4, 4, 1, 1, 7, 1, 1, 5, 1, 4, 50, 21, 7, 28, 2, 4, 1, 2, 2, 1, 1, 1, 4, 3, 2, 11, 5, 4, 19, 1, 2, 1, 3, 10, 1, 14, 1, 1, 18, 6, 1, 14, 9, 1, 6, 1, 1, 2, 3, 1, 3, 1, 2, 7, 16, 2, 1, ...$]$.

The correct match for K, d are found to be:

K = 313502095308421820319312187072648398207
503241292725274374998886089540461751327
79281610521901824857

d = 305923991492197993569398452307744493597
067975876384134442848163832956575217972
52658495003050969.

This reveals the prime factors:

p = 884234029640213583459288805558955205223
615402467727593575790821189784625657565
240795770464454149022686841858476837415
4372317409696092611240744813864770711

q = 884234029640213583417486079216384023929
224609757928703058502403539769379524876
433776448394874081644022996403747254411
2092849602164528666613060910519239523.

The values δ and β are also calculated,
$\delta \approx 0.306878 < \dfrac{5}{16}$ and $\beta \approx 0.437234 < \dfrac{7}{16}$.
This shows that the range of weak keys can be found 5 bits beyond the proven value.

Example 3: Consider a pragmatic scenario of the mutual authentication between the smart card and terminal. To authenticate the smart card, suppose the terminal sends a (64-bit) random number *Rnd* as a challenge to the smart card. Assume that the public key pair (E, N) of the smart card is given in Example 2. Since d is known, the intercepted ciphertext C can be decrypted, as follows:

$$
\begin{aligned}
C = {} & 5878781249236288185620639889910625576 29\\
& 4205251964038408117731324230565307358 64\\
& 5954899594885138872384994940515706660 61\\
& 4433982924956560790719725768974544263 33\\
& 3138539842889788371310157721547248776 93\\
& 5910228342876001420504171616359054938 71\\
& 9000476861535278772204190143550232294 35\\
& 81742444951964039791008036945856572
\end{aligned}
$$

$Rnd \equiv C^d \equiv 14366806732082741851 \mod (N).$

4 CONCLUSIONS

Despite the fact that there exist efficient attacks on the scheme, RSA remains as the primary choice for security algorithm in many areas of technology today. RSA keys are used on the web for protecting webmail, online banking, and other sensitive online services. A recent security analysis was performed on RSA keys found on the web in order to test the validity of the assumption that different random choices are made each time keys are generated, revealed that the vast majority of public keys work as intended. However, it was discovered that two out of every one thousand RSA moduli that were collected offer no security leading to the conclusion that the validity of the assumption is questionable (Lenstra et al., 2011).

In this paper we investigated for which values of the variables σ and $\Delta = |p-q|$, RSA which uses public keys of the special structure $E = e + \sigma\varphi(N)$, where $e < \varphi(N)$, is insecure against cryptanalysis. Adding multiples of $\varphi(N)$ either to e or to d is called Exponent Blinding and it is widely used especially in case of encryption schemes or digital signatures implemented in portable devices such as smart cards (Schindler and Itoh, 2011). We show that an extension of de Weger's attack from public keys $e < \varphi(N)$ to $E > \varphi(N)$ is possible if the security parameter σ satisfies $\sigma \leq N^{\frac{1}{2}}$. This attack is efficient since the continued fraction algorithm runs in polynomial time in $\log N$. With a 1024-bit RSA modulus N, the Attack Algorithm takes as little as 10 *ms* to factor N. Moreover, we provided a rigorous proof for the maximum value of σ that our attack will succeed, namely $\sigma \leq N^{\frac{1}{2}}$. However, from a theoretical point of view, if $|p-q|$ is slightly larger than $N^{\frac{1}{4}}$, then the attack will work up to $\sigma < N$, since $d \simeq \dfrac{N^{\frac{1}{2}}}{\sqrt{1+N}} \simeq 1$. Hence, to achieve security against our attack, it is recommended that σ to be chosen $\sigma \simeq N$.

None of the attacks discussed in this paper found a weakness in the construction of the RSA cryptosystem itself. The reason that we were able to demonstrate a successful attack is because users make bad security decisions. Choosing a small secret key d, for instance, is a bad security decision. As we have seen, some users make their decisions as a form of trade-off between security and computational costs. These users are not better off than those who possess a perception of futility regarding security.

ACKNOWLEDGEMENTS

We would like to thank the anonymous referees of this paper who helped us a lot to improve it.

REFERENCES

Boneh, D. and Durfee, G. (2000). Cryptanalysis of rsa with private key d less than $n^{0.292}$. In *Information Theory, IEEE Transactions, 46: 1339 - 1349*.

Crandall, R. and Pomerance, C. (2005). *Prime Numbers: A Computational Perspective*. Springer. ISBN 0-387-25282-7.

Dujell, A. and Ibrahimpasic, B. (2008). On worleys theorem in diophantine approximations. In *Ann. Math. Inform. 35 (2008), 61-73*.

Goldreich, O. (2008). *Computational Complexity: A conceptual Perspective*. Cambridge University Press, New York, 1st edition.

Hardy, G. H. and Wright, E. M. (2008). *An introduction to the theory of numbers*. Oxford University Press, Oxford, 6th edition.

Hinek, J. (2010). *Cryptanalysis of RSA and its variants*. CRC Press, New York, 1st edition.

Joux, A. (2009). *Algorithmic Cryptanalysis*. CRC Press, New York, 1st edition.

Lenstra, A. K., Hughes, J. P., Augier, M., Bos, J. W., Kleinjung, T., and Wachte, C. (2011). Ron was wrong, whit is right. In *Available at: http://eprint.iacr.org/2012/064*.

Lenstra, A. K. and Verheul, E. R. (2000). Selecting cryptographic key sizes. In *PKC2000: p. 446-465, 01/2000*.

May, A. (2003). *New RSA vulnerabilities using Lattice Reduction Methods*. PhD thesis, University of Paderborn.

McKee, J. (1999). Speeding fermat's factoring method. In *Mathematics of Computation, 68:1729-1737*.

Rivest, R., Shamir, A., and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. In *Communications of the ACM, 21 Issue 2: 120 - 126*.

Schindler, W. and Itoh, K. (2011). Exponent blinding does not always lift (partial) spa resistance to higher-level security. In *Lecture Notes in Computer Science, Volume 6715/2011, 73-90*.

Schneier, B. (1996). *Applied Cryptography: Protocols, Algorithms and Source Code in C*. John Willey, New York, 2nd edition.

Shoup, V. (2009). Number theory library. http://www.shoup.net/ntl/.

Weger, B. (2002). Cryptanalysis of rsa with small prime difference. In *IACR Eprint archive*.

Wiener, M. (1990). Cryptanalysis of short rsa secret exponents. In *Information Theory, IEEE Transactions,36: 553 - 558*.