FACTORING CRYPTOSYSTEM MODULI WHEN THE CO-FACTORS DIFFERENCE IS BOUNDED

Omar Akchiche[1] and Omar Khadir[2]

[1,2]Laboratory of Mathematics, Cryptography and Mechanics, Fstm, University of Hassan II Mohammedia-Casablanca, Morocco

omar.akchiche@hotmail.fr
khadir@hotmail.com

ABSTRACT

Let p, q be two large primes and N= pq *. We show, in this paper, that if* $|p-q| \leq N2^{\frac{k+5}{4}}$ *where* k *is the bit-size of* n *and* $N \in \mathbb{N}$*, then we can compute efficiently the integers* p *and* q *in at most* N^2 *comparisons. Our approach can be used to build attacks against RSA or Rabin cryptosystems.*

KEYWORDS

Integer factorization problem, RSA, Rabin cryptosystem, Public key cryptography.

1. INTRODUCTION

Factoring large integers is a central issue in cryptography. No efficient deterministic algorithm is known. Widely used cryptographic protocols like RSA [1], Rabin [2] system or Saryazdi [3] digital signature rely on this fact.

In many cryptosystems, each user must randomly choose two large prime numbers p and q to produce his own keys. These integers have to be sufficiently large to ensure that it is not computationally possible for anyone to factor the modulus $n = pq$. Generally, the running time for generating primes takes the most important part in the total running time. Menezes and all. [4, p. 133] give several algorithms for prime number generation and primality testing. Also, in [5], the authors made experimental tests and concluded by suggesting some rapid procedures.

In literature, there exist various integer factorization methods, but they are not efficient. The oldest and simplest one is the trial divisions. Fermat [6, p. 143] proposed a technique for factoring integers that are product of two primes which are close to one another. The continued fraction algorithm [7] was developed in 1931. Some decades later, John Pollard conceived his $p-1$ and ρ methods [8,9] respectively in 1974 and 1975. At the end of 1970s, with the advent of the public key cryptography [10,1,2], integer factorization problem becomes of crucial importance. Numerous papers, proposing ingenious and sophisticated methods, were published. Pomerance [11] discovered the quadratic sieve algorithm in 1984. Less than two years later, Lenstra [12] suggested to factor large numbers by means of finite elliptic curves. Today, the fastest known algorithm is the General Number Field Sieve (GNFS) [13, p. 103]. It was invented by Pollard in 1988 and allows to factor natural integers with more than 110 digits. Stinson [14, p. 232] has

DOI : 10.5121/ijitmc.2013.1301

evoked the possibility of factoring the RSA modulus if the two factors are too close. In 1999, Boneh and al. [15] described a polynomial time algorithm for factoring $n = p^r q$ when the exponent r is large. Some years later, in 2007, Coron and May [16] presented the first deterministic algorithm for factoring the RSA modulus in polynomial time, but they used the public and the secret key pair (e, d).

Our work is devoted to present original results related to integer factorization problem. Indeed, we improve many statements established in two previous articles [17,18]. Furthermore, our approach can be used to build attacks against cryptosystems like RSA [1], Rabin [2] or Saryazdi digital signature [3].

The paper is organised as follows. In section 2, we recall the main facts stated in papers [17] and [18]. In section 3, we present our own results and we conclude in section 4.

Throughout all the sequel, we will use standard notations. In particular $\mathbb{N}$ is the set of all natural integers $0,1,2,3, \ldots$ and $\mathbb{N}^* = \mathbb{N} - \{0\}$. The largest integer which does not exceed the real x is denoted by $\lfloor x \rfloor$. It is also the integer part and the floor of x. Thus we have $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$. The bit-size of a positive integer n is the number of bits in its binary representation. So, the bit-size of n is $k \Leftrightarrow n = \sum_{i=0}^{k-1} a_i 2^i$ with every $a_i \in \{0,1\}$ and $a_{k-1} = 1$. Moreover, the bit-size of n satisfies the relation$2^{k-1} \leq n < 2^k$. Two positive integers p and q are said to be co-factors of n if $n = pq$.

We start by recalling some known results.

2. PRELIMINARIES

In this section, we recall results established in 2008 and 2010 and described in papers [17] and [18]. More precisely, we review sufficient conditions under which one can factor $n = pq$ where p, q are co-factors not necessary prime but close to each other. For the sake of completeness, we give all the proofs. First we present a statement published in [17]. Before that, we need the following lemma.

Lemma 1. [17] Let $n < m$ be two elements of $\mathbb{N}^*$ and let $\alpha_{n,m}$ denotes the number of perfect squares x^2 such that $n < x^2 \leq m$. Then we have: $\alpha_{n,m} < \frac{m-n}{\sqrt{m}+\sqrt{n}} + 1$.

Proof. Consider the set $E_n = \{x^2 \in \mathbb{N} \mid x^2 \leq n\}$. Since E_n is also $\{x \in \mathbb{N} \mid x \leq \sqrt{n}\}$, its cardinality is $\lfloor \sqrt{n} \rfloor + 1$, and then $\alpha_{n,m} = \lfloor \sqrt{m} \rfloor - \lfloor \sqrt{n} \rfloor$. If we put $k = \lfloor \sqrt{n} \rfloor$ and $l = \lfloor \sqrt{m} \rfloor$ which means that $k \leq \sqrt{n} < k + 1$ and $l \leq \sqrt{m} < l + 1$, we obtain $l \leq \sqrt{m}$ and $-k < 1 - \sqrt{n}$. Hence $\alpha_{n,m} = l - k < \sqrt{m} - \sqrt{n} + 1 = \frac{m-n}{\sqrt{m}+\sqrt{n}} + 1$.

□

The following theorem was one of the main results in paper [17].

Theorem 1. [17] Let $n \in \mathbb{N}$ be a composite integer whose bit-size is k. If its two prime factors p and q satisfy the inequality:

$$|q - p| \leq 2^{\frac{k+5}{4}} \tag{1}$$

then we can compute them efficiently.

Proof. Without loss of generality, we assume that $2 < p < q$. As the prime factors p and q are odd, we put $q = p + 2i$ where $i \in \mathbb{N}$. Since $n = pq$, $n + i^2 = (p + i)^2$. By relation (1), $|q - p| \leq 2^{\frac{k+5}{4}}$. It follows that $i = \frac{q-p}{2} \leq 2^{\frac{k+1}{4}}$ and then $i^2 \leq 2^{\frac{k+1}{2}}$. Let $m = n + i^2$ where $i > 0$. We have $m > n$. By Lemma 1, the number $\alpha_{n,m}$ of perfect squares between n and m satisfies the inequality $\alpha_{n,m} < \frac{i^2}{\sqrt{n+i^2}+\sqrt{n}} + 1$. We deduce that $\alpha_{n,m} < \frac{i^2}{2\sqrt{n}} + 1$. The bit-size of n is k, so $n \geq 2^{k-1}$. Thus $2\sqrt{n} \geq 2^{\frac{k+1}{2}}$. Therefore $\alpha_{n,m} < \frac{2^{\frac{k+1}{2}}}{2^{\frac{k+1}{2}}} + 1 = 2$. However $\alpha_{n,m}$ is an integer, so $\alpha_{n,m} = 1$ This means that the only perfect squares between n and m is $m = n + i^2 = (p + i)^2$. But the first perfect square greater than n is $n_0^2 = (\lfloor\sqrt{n}\rfloor + 1)^2$. This allows us to compute the factors p and q. Indeed, since $n_0^2 - n = i^2$ is a perfect square, $n = (n_0 - i)(n_0 + i)$. Then, we have $p = n_0 - i$ and $q = n_0 + i$. Hence $p = \lfloor\sqrt{n}\rfloor - i + 1$ and $q = \lfloor\sqrt{n}\rfloor + i + 1$.

□

Now we move to results published in paper [18]. But first, we give two definitions.

Definition 1. [18] Let $n \in \mathbb{N}$ be a composite integer. The minimal distance $d(n)$ of n is the smallest distance between its co-factors:

$$d(n) = \{|p - q|,\ p, q \in \mathbb{N}, n = pq\} \tag{2}$$

Next fact is easy to prove.

Theorem 2. [18] For every composite integer $n \in \mathbb{N}$, there exists a unique couple (p, q) of divisors of n such that $n = pq$ and $d(n) = |p - q|$.

Definition 2. [18] Let $n \in \mathbb{N}$ be a composite integer. The unique couple of positive integers (p, q) such that $n = pq$ and $d(n) = |p - q|$ is called the *weak decomposition* of n.

For all the proofs below, we denote by $n = pq$ the odd natural integer to be factorized where (p, q) is its weak decomposition and $d(n)$ is its minimal distance as stated in relation (2). For simplicity, we assume that $2 < p < q$. We also define$m = n + i^2$ such that $q - p = d(n) = 2i$, $i \in \mathbb{N}^*$ since n is odd. According to previous notations, it is readily seen that $m = (p + i)^2$. Observe that as $i > 0$, $m > n$. Furthermore, we let $\alpha_{n,m}$ be the number of perfect squares between n and m.
The next theorem was the main result in [18]. In the sequel, the term *comparison* means the operation consisting of checking if a given natural integer is a perfect square or not.

Theorem 3. [18] For every composite odd integer $n \in \mathbb{N}$ whose bit-size is k, if there exists a number l such that the minimal distance of n verifies:

$$d(n) \leq 2^{\frac{k+5+2l}{4}} \tag{3}$$

then one can find the weak decomposition of n in at most 2^l comparisons.

Proof. By Lemma 1, since $\alpha_{n,m}$ is the number of perfect squares x^2 such that $n < x^2 \leq m$, $\alpha_{n,m} < \frac{m-n}{\sqrt{m}+\sqrt{n}} + 1 < \frac{i^2}{2\sqrt{n}} + 1$. On the other hand, by relation (3) $d(n) \leq 2^{\frac{k+5+2l}{4}}$, so $i^2 \leq 2^{\frac{k+1+2l}{2}}$. As k is the bit-size of n, $n \geq 2^{k-1}$. We obtain $\alpha_{n,m} < \frac{2^{\frac{k+1+2l}{2}}}{2.2^{\frac{k-1}{2}}} + 1 < 2^l + 1$. Since $\alpha_{n,m}$ is a natural integer, it is clear that $\alpha_{n,m} \leq 2^l$. The only 2^l perfect squares immediately greater than n are $(\lfloor\sqrt{n}\rfloor + j)^2, 1 \leq j \leq 2^l$. As $n + i^2$ is a perfect square between n and m, there exists necessary an integer $j_0 \in \{1,2, \dots , 2^l\}$ such that:

$$n + i^2 = (\lfloor\sqrt{n}\rfloor + j_0)^2$$

This relationship implies that: $n = \left(\lfloor\sqrt{n}\rfloor + j_0 - i\ \right)(\lfloor\sqrt{n}\rfloor + j_0 + i\ )$. If we put $p_1 = \left(\lfloor\sqrt{n}\rfloor + j_0 - i\ \right)$ and $q_1 = \left(\lfloor\sqrt{n}\rfloor + j_0 + i\ \right)$, then $q_1 - p_1 = 2i = d(n)$. Therefore the couple (p_1, q_1) is a weak decomposition of n. However, by Theorem 2, $p = p_1$ and $q = q_1$which ends the computation of the two factors p and q.

We find j_0 by making at most 2^l comparisons since $j_0 \in \{1,2, \dots , 2^l\}$.

□

In the following section, we improve and extend the main results established in papers [17] and [18].

3. OUR RESULTS

In this section, we present our main contribution by extending Theorem 1. First, we need a slightly modified version of Lemma 1.

Lemma 2. If $n < m$ are two elements of $\mathbb{N}^*$ and if $\alpha_{n,m}$ denotes the number of perfect squares x^2 such that $n < x^2 \leq m$. Then we have:

$$\frac{m-n}{\sqrt{m}+\sqrt{n}} - 1 < \alpha_{n,m} < \frac{m-n}{\sqrt{m}+\sqrt{n}} + 1 \qquad (4)$$

Proof. The right inequality in relation (4) was proved in Lemma 1. It is not difficult to see that $\alpha_{n,m} = \lfloor\sqrt{m}\rfloor - \lfloor\sqrt{n}\rfloor$. If we put $k = \lfloor\sqrt{n}\rfloor$ and $l = \lfloor\sqrt{m}\rfloor$ which means that $k \leq \sqrt{n} < k + 1$ and $l \leq \sqrt{m} < l + 1$, we obtain $l > \sqrt{m} - 1$ and $-k \geq -\sqrt{n}$. Hence $\alpha_{n,m} = l - k > \sqrt{m} - \sqrt{n} - 1 = \frac{m-n}{\sqrt{m}+\sqrt{n}} - 1$which ends the proof. Note that we also have $|\alpha_{n,m} - \frac{m-n}{\sqrt{m}+\sqrt{n}}| < 1$.

□

Throughout the sequel, we make use of the following lemma.

Lemma 3. Let n be a composite odd integer. The first natural integer j such that $\left(\lfloor\sqrt{n}\rfloor + j\right)^2 - n$ is a perfect square is exactly $\alpha_{n,m}$. Moreover, if one can compute $\alpha_{n,m}$, then it is possible to find the weak decomposition of n.

Proof. The number of perfect squares between n and m is $\alpha_{n,m}$. Thus, the perfect squares x^2 such that $n < x^2 \leq m$ have the form $\left(\lfloor\sqrt{n}\rfloor + j\right)^2, j \in \{1,2, \dots , \alpha_{n,m}\}$. The largest one is $\left(\lfloor\sqrt{n}\rfloor + \alpha_{n,m}\right)^2$. Hence, we must have $m = \left(\lfloor\sqrt{n}\rfloor + \alpha_{n,m}\right)^2$. Therefore $\left(\lfloor\sqrt{n}\rfloor + \alpha_{n,m}\right)^2 - n$ is a perfect square i^2. The first assertion is then proved. In order to justify the second one, assume that we know $\alpha_{n,m}$, Since $n + i^2 = \left(\lfloor\sqrt{n}\rfloor + \alpha_{n,m}\right)^2$, we deduce that $n = \left(\lfloor\sqrt{n}\rfloor + \alpha_{n,m} - i\right)(\lfloor\sqrt{n}\rfloor + \alpha_{n,m} + i)$. Let $p_1 = \lfloor\sqrt{n}\rfloor + \alpha_{n,m} - i$ and $q_1 = \lfloor\sqrt{n}\rfloor + \alpha_{n,m} + i$. As $q_1 - p_1 = 2i = d(n)$, the couple (p_1, q_1) is a weak decomposition of n. Consequently, by Theorem 2, $p = p_1$ and $q = q_1$ which ends the computation of the two co-factors of n.

□

Now, we give our first main result: an extension of Theorem 1.

Theorem 4. For every composite odd integer $n \in \mathbb{N}$ whose bit-size is k, if there exists a positive number N such that the minimal distance of n verifies:

$$d(n) \leq N 2^{\frac{k+5}{4}} \tag{5}$$

then one can find the weak decomposition of n in at most N^2 comparisons.

Proof. As $d(n) \leq N 2^{\frac{k+5}{4}}$, $i = \frac{d(n)}{2} = N 2^{\frac{k+1}{4}}$, and then $i^2 \leq N^2 2^{\frac{k+1}{2}}$. Since by Lemma 1, $\alpha_{n,m} < \frac{i^2}{2\sqrt{n}} + 1$, it follows that $\alpha_{n,m} < N^2 \; \frac{2^{\frac{k+1}{2}}}{2^{\frac{k+1}{2}}} + 1$. Therefore $\alpha_{n,m} < N^2 + 1$. But $\alpha_{n,m}$ is a natural integer, so $\alpha_{n,m} \leq N^2$. By Lemma 3, in order to compute $\alpha_{n,m}$, one must determine the first positive integer j, $j \leq N^2$, such that $\left(\lfloor\sqrt{n}\rfloor + j\right)^2 - n$ is a perfect square. Thus, for this purpose, we need at most N^2 comparisons. By the same Lemma 3, once $\alpha_{n,m}$ is known, we are able to find the weak decomposition of n.

□

Remark 1. Our result is also an improvement of Theorem 3 from paper [18] by taking $N = 2^{\frac{l}{2}}$, $l \in \mathbb{N}^*$.

Theorem 4 leads to the following efficient algorithm where comments are delimited with braces.

Algorithm:

Input: A composite odd positive integer n.
Output: The weak decomposition (p, q) of n.

```
1. input($n$); {$n$ is the composite natural integer to be factored}
2. $N \longleftarrow 1$; {We initialise the value of $N$ in relation (5)}
3. flag $\longleftarrow 0$; {The program ends when flag becomes 1}
4. while flag $= 0$ do
4.1. $j \longleftarrow (N-1)^2 + 1$; {We initialise the value of $j$. We look for $j$ such that $\left(\lfloor\sqrt{n}\rfloor + j\right)^2 - n$ is a perfect square}
4.2. while $j \leq N^2$ and flag $= 0$ do
4.2.1 $M \longleftarrow \lfloor\sqrt{n}\rfloor + j$;
4.2.2 $S \longleftarrow M^2 - n$;
4.2.3 if $S$ is a perfect square then {Here $S = \left(\lfloor\sqrt{n}\rfloor + j\right)^2 - n$}
4.2.3.1 $i \longleftarrow \sqrt{S}$;
4.2.3.2 $p \longleftarrow M - i$; {$p$ is the first co-factor of $n$}
4.2.3.3 $q \longleftarrow M + i$; {$q$ is the second co-factor of $n$}
4.2.3.4 flag $\longleftarrow 1$; {We stop the program since $n$ is factored by previous instructions}
4.2.3.5 output $(p, q)$; {The algorithm computes the weak decomposition of $n$}
4.2.4 $j \longleftarrow j + 1$; {We increment $j$}
4.3 $N \longleftarrow N + 1$; {We enlarge the coefficient $N$ such that $|p - q| \leq N 2^{\frac{k+5}{4}}$ }
```

Next corollary improves Theorem 4 if more information is known.

Corollary 1. For every composite odd integer $n \in \mathbb{N}$ whose bit-size is k, if N is the smallest positive integer such that:

$$d(n) \leq N2^{\frac{k+5}{4}} \tag{6}$$

with $N < 2^{\frac{k+1}{4}}$, then we can determine the weak decomposition of n in at most $N^2 - \left\lfloor\frac{(N-1)^2}{2\sqrt{2}}\right\rfloor + 1$ comparisons.

Proof. We proved in Theorem 4 that $\alpha_{n,m} < N^2$, let us here show that $\alpha_{n,m} \geq \left\lfloor\frac{(N-1)^2}{2\sqrt{2}}\right\rfloor$. The bit-size of n is k, so $n \geq 2^{k-1}$ and then $2\sqrt{n} \geq 2^{\frac{k+1}{2}}$. By hypothesis (6) $i = \frac{d(n)}{2} \leq N2^{\frac{k+1}{4}}$. We assumed that $N < 2^{\frac{k+1}{4}}$, so $N2^{\frac{k+1}{4}} < 2^{\frac{k+1}{2}}$. Therefore $i < 2\sqrt{n}$. The fact that k is the bit-size of n leads to $n < 2^k$ and then $2\sqrt{n} < 2^{\frac{k+2}{2}}$. This implies that $i + 2\sqrt{n} < 2.\,2^{\frac{k+2}{2}} = 2^{\frac{k+4}{2}}$. So we obtain $\frac{1}{i+2\sqrt{n}} > \frac{1}{2^{\frac{k+4}{2}}}$. Recall that N is the smallest integer which satisfies inequality (6). That means $d(n) > (N-1)2^{\frac{k+5}{4}}$. As $i = \frac{d(n)}{2}$, $i > (N-1)2^{\frac{k+1}{4}}$ and then $i^2 > (N-1)^2 2^{\frac{k+1}{2}}$. By Lemma 2, $\alpha_{n,m} > \frac{i^2}{i+2\sqrt{n}} - 1$. Hence $\alpha_{n,m} > \frac{(N-1)^2 2^{\frac{k+1}{2}}}{2^{\frac{k+4}{2}}} - 1 = \frac{(N-1)^2}{2\sqrt{2}} - 1$. Since $\alpha_{n,m}$ is an integer, we must have $\alpha_{n,m} \geq \left\lfloor\frac{(N-1)^2}{2\sqrt{2}}\right\rfloor$. We proved that $\left\lfloor\frac{(N-1)^2}{2\sqrt{2}}\right\rfloor \leq \alpha_{n,m} \leq N^2$. By Lemma 3, to compute $\alpha_{n,m}$, we have to determine the first integer j such that $\left(\lfloor\sqrt{n}\rfloor + j\right)^2 - n$ is a perfect square. We are sure that $\left\lfloor\frac{(N-1)^2}{2\sqrt{2}}\right\rfloor \leq j \leq N^2$. It is clear that we will need at most $N^2 - \left\lfloor\frac{(N-1)^2}{2\sqrt{2}}\right\rfloor + 1$ comparisons. Then, by the same Lemma 3, knowing $\alpha_{n,m}$, we can find the weak decomposition of n.

□

Example 1. Let us take $\mathrm{n} = 84009841$ as in paper [19]. With the help of Maple software, the first positive integer j for which $\left(\lfloor\sqrt{n}\rfloor + j\right)^2 - n$ is a perfect square is $\mathrm{j} = 370$.Therefore the two factors of n are $\mathrm{p} = 6907$ and $\mathrm{q} = 12163$. On another hand, the first natural integer N such that $d(n) \leq N2^{\frac{k+5}{4}}$ is $\mathrm{N} = 21$, and we check that j is belonging to the interval $\left[\left\lfloor\frac{(N-1)^2}{2\sqrt{2}}\right\rfloor, N^2\right]$.

In the next result, we improve Theorem 3 under certain assumptions. But, first we need the following theorem.

Theorem 5. For every composite odd integer $n \in \mathbb{N}$ whose bit-size is k, if we can find a natural integer l and a positive real x such that:

$$2^{\frac{k+8+2x}{4}} < d(n) \leq 2^{\frac{k+5+2l}{4}} \tag{7}$$

with $2l < k+1$, then one can find the weak decomposition of n in at most $2^l - \lfloor 2^x \rfloor + 1$ comparisons.

Proof. In the proof of Theorem 3, we have seen that $\alpha_{n,m} \leq 2^l$. Now we show that $\alpha_{n,m} \geq \lfloor 2^x \rfloor$. As k is bit-size of n, $n \geq 2^{k-1}$ and then $2\sqrt{n} \geq 2^{\frac{k+1}{2}}$. Since $d(n) \leq 2^{\frac{k+5+2l}{4}}$, $i = \frac{d(n)}{2} \leq 2^{\frac{k+1+2l}{4}}$. By hypothesis $2l < k+1$, thus $2^{\frac{k+1+2l}{4}} < 2^{\frac{k+1}{2}}$. Therefore $i < 2\sqrt{n}$. Moreover, k is the bit-size of n, so $2\sqrt{n} < 2^{\frac{k+2}{2}}$. It follows that $i + 2\sqrt{n} < 2.\,2^{\frac{k+2}{2}} < 2^{\frac{k+4}{2}}$. We then get $\frac{1}{i+2\sqrt{n}} > \frac{1}{2^{\frac{k+4}{2}}}$. Since, by relation (7), $d(n) > 2^{\frac{k+8+2x}{4}}$, we have $i = \frac{d(n)}{2} > 2^{\frac{k+4+2x}{4}}$. So, we deduce that $i^2 > 2^{\frac{k+4+2x}{2}}$. By Lemma 2, $\alpha_{n,m} > \frac{m-n}{\sqrt{m}+\sqrt{n}} - 1$. Therefore $\alpha_{n,m} > \frac{i^2}{i+2\sqrt{n}} -1$. Finally, we obtain $\alpha_{n,m} > \frac{2^{\frac{k+4+2x}{2}}}{2^{\frac{k+4}{2}}} - 1 > 2^x - 1$. But $\alpha_{n,m}$ is a integer, so $\alpha_{n,m} \geq \lfloor 2^x \rfloor$. We proved that $\lfloor 2^x \rfloor \leq \alpha_{n,m} \leq 2^l$. By Lemma 3, the integer $\alpha_{n,m}$ verifies that $\left(\lfloor\sqrt{n}\rfloor + \alpha_{n,m}\right)^2 - n$ is a perfect square. That means that in order to compute $\alpha_{n,m}$, one must checks if $\left(\lfloor\sqrt{n}\rfloor + j\right)^2 - n$ is a perfect square for j such that $\lfloor 2^x \rfloor \leq j \leq 2^l$. Obviously, we need at most $2^l - \lfloor 2^x \rfloor + 1$ comparisons. Then, by the same Lemma 3, once we know $\alpha_{n,m}$, we can find the weak decomposition of n.

□

The following corollary, our second main result, slightly improves Theorem 3 [18]. It reduces the number of comparisons to perform.

Corollary 2. For every composite odd integer $n \in \mathbb{N}$ whose bit-size is k, if we can find the smallest positive integer l such that:

$$d(n) \leq 2^{\frac{k+5+2l}{4}} \tag{8}$$

With $2l < k + 1$, then one can find the weak decomposition of n in at most $2^l - \left\lfloor 2^{l-\frac{5}{2}} \right\rfloor + 1$ comparisons.

Proof. We share the value of the exponent of the first term in relation (7) into two part: $2 + 8 + 2\text{x} = \text{x} + 5 + (3 + 2\text{x})$. Since l is the smallest positive integer that satisfies the inequality (8), $d(n) > 2^{\frac{k+5+2(l-1)}{4}}$. Therefore, in order to apply Theorem 5, we must have $3 + 2\text{x} = 2(\text{l} - 1)$. In other words, $x = l - \frac{5}{2}$. Hence, the assertion is proved.

□

The following theorem enlarges the bound in relation (3) without adding much cost.

Theorem 6. For every composite odd integer $n \in \mathbb{N}$ whose bit-size is k, if there exists a positive integer l such that the minimal distance of l verifies:

$$d(n) \leq 2^{\frac{k+5+2l}{4}} + 2^{\frac{k+5-2l}{4}} \tag{9}$$

with $2l < k + 5$, then one can find the weak decomposition of n in at most $2^l + 3$ comparisons.

Proof. For simplicity, let $B = 2^{\frac{k+5-2l}{4}}$. So the hypothesis (9) becomes $d(n) < 2^{\frac{k+5+2l}{4}} + B$. As $i = \frac{d(n)}{2}$, $i \leq 2^{\frac{k+1+2l}{4}} + \frac{B}{2}$. Therefore, it is clear that $i^2 \leq 2^{\frac{k+1+2l}{2}} + \frac{B^2}{4} + B2^{\frac{k+1+2l}{4}}$. The bit-size of n is k, so $\frac{1}{2\sqrt{n}} < \frac{1}{2^{\frac{k+1}{2}}}$. Since, by Lemma 1, $\alpha_{n,m} < \frac{i^2}{2\sqrt{n}} + 1$, we have:

$$\alpha_{n,m} < \frac{2^{\frac{k+1+2l}{2}}}{2^{\frac{k+1}{2}}} + \frac{B^2}{4.2^{\frac{k+1}{2}}} + B\frac{2^{\frac{k+1+2l}{4}}}{2^{\frac{k+1}{2}}} + 1$$

If we substitute B with its value, then we get $\alpha_{n,m} < 2^l + \frac{1}{2^l} + 2 + 1$. Recall that $\alpha_{n,m}$is an integer, so $\alpha_{n,m} \leq 2^l + 3$. Consequently, by Lemma 3, in order to find a natural integer j such that $\left(\lfloor\sqrt{n}\rfloor + j\right)^2 - n$ is a perfect square, we need at most $2^l + 3$ comparisons. By the same Lemma 3, it is possible to determine the weak decomposition of n since $j = \alpha_{n,m}$, which ends the proof.

□

4. Conclusion

In this paper, we presented new conditions under which one can factor a large composite integer and we gave an extension of previous results published in [17, 18]. Our work can be applied to build attacks against several cryptosystems based on the hardness of integer factorization like RSA [1] and Rabin [2] algorithms or like Saryazdi digital signature [3]. We recommend to cryptosystem designers to avoid all these insecure composite modulus mentioned in our results.

References

[1] R. Rivest & A. Shamir & L. Adeleman, (1978) “A method for obtaining digital signatures and public key cryptosystems”, Communications of the ACM, Vol. 21, pp. 120-126. .

[2] M. O. Rabin, (1979) “Digitalized signatures and public key function as intractable as factoring”, MIT/LCS/TR, Vol. 212.

[3] S. Saryazdi, (1990) “An extension to ElGamal public key cryptosystem with a new signature scheme”, Proceedings of the 1990 Bilkent International Conference on New Trends in Communication, Control, and Signal Processing, North Holland: Elsevier Science Publishers, pp. 195-198.

[4] A. J. Menezes & P. C. van Oorschot & S. A. Vanstone, (1997) “Handbook of Applied Cryptography”, CRC Press, Boca Raton, Florida.[5]O. Khadir & L. Szalay, (2009) “Experimental results on probable primality”, Acta Univ. Sapientiae, Math., 1, no. 2, pp. 161-168.Available at http://www.emis.de/journals/AUSM/C1-2/math2-6.pdf

[6] N. Kobliz, (1994) “A course in Number Theory and Cryptography”, Graduate Texts in Mathematics, Springer-Verlag, New York.

[7] D. H. Lehmer & R. E. Powers, (1931) “On factoring large numbers”, Bull. Amer. Math. Soc. Vol. 37 (10), pp. 770-776.

[8] J. M. Pollard, (1974) “Theorems of factorization and primality testing”, Proceedings of Cambridge Philosophical Society, Vol. 76, pp. 521-528.

[9] J. M. Pollard, (1975) “A Monte Carlo method for factorization”, BIT, Vol. 15, pp. 331-334.

[10] W. Diffie & M. E. Hellman, (1976) “New directions in cryptography”, IEEE Transactions on Information Theory, Vol. IT-22, pp. 644-654.

[11] C. Pomerance, (1985) “The quadratic sieve factoring algorithm”, In Proc. of Eurocrypt'84, Workshop on Advances in Cryptology: Theory and Application of Cryptographic Techniques, Springer-Verlag New York, pp. 169-182.

[12] H. W. Lenstra, (1987) “Factoring integers with elliptic curves”, Annals of Mathematics, Vol. 126 (2), pp. 649-673.

[13] A. K. Lenstra & H. W. Lenstra, Jr., (1993) “The development of the Number Field Sieve”, Series Lecture Notes in Mathematics, Vol. 1554, Springer-Verlag.

[14] D. R. Stinson, (2006) “Cryptography, Theory and Practice”, 3rd Edition, Chapman & Hall/CRC.

[15] D. Boneh & G. Durfee & N. A. Howgrave-Graham, (1999) “Factoring n=p^r q for large r”, in Proceeding of Crypto'99, LNCS, Vol. 1666, Spring-Verlag, Berlin, pp. 326-337.

[16] J. S. Coron & A. May, (2007) “Deterministic polynomial-time equivalence of computing the RSA secret key and factoring”, Journal of Cryptology, Vol. 20, pp.39-50.

[17] O. Khadir, (2008) “Algorithm for factoring some RSA and Rabin moduli”, J. Discrete Math. Sci. Cryptography, Vol. 11 (5), pp. 537-543.

[18] O. Khadir & L. Szalay, (2010) “Sufficient conditions for factoring a class of large integers”, J.. Interdiscip. Math., Vol. 13, No. 1, pp. 95-103.

[19] J. McKee, (1999) “Speeding Fermat's factoring method”, Mathematics of Computation, Vol.68, pp. 1729-1737.