New Formulas for Semi-Primes. Testing, Counting and Identification of the n^{th} and next Semi-Primes

Issam Kaddoura, Khadija Al-Akhrass
Department of Mathematics, school of arts and sciences
Lebanese International University
Saida, Lebanon

Samih Abdul-Nabi
Department of computers and communications engineering,
Lebanese International University
Beirut, Lebanon
Email: Samih.abdulnabi [AT] liu.edu.lb

Abstract—**In this paper we give a new semiprimality test and we construct a new formula for $\pi^{(2)}(N)$, the function that counts the number of semiprimes not exceeding a given number N. We also present new formulas to identify the n^{th} semiprime and the next semiprime to a given number. The new formulas are based on the knowledge of the primes less than or equal to the cube roots of $N : P_1, P_2 \ldots . P_{\pi(\sqrt[3]{N})} \leq \sqrt[3]{N}$.**

Keywords-component; prime, semiprime, n^{th} semiprime, next semiprime

I. INTRODUCTION

Securing data remains a concern for every individual and every organization on the globe. In telecommunication, cryptography is one of the studies that permit the secure transfer of information [1] over the Internet. Prime numbers have special properties that make them of fundamental importance in cryptography. The core of the Internet security is based on protocols, such as SSL and TSL [2] released in 1994 and persist as the basis for securing different aspects of today's Internet [3].

The Rivest-Shamir-Adleman encryption method [4], released in 1978, uses asymmetric keys for exchanging data. A secret key S_k and a public key P_k are generated by the recipient with the following property: A message enciphered by P_k can only be deciphered by S_k and vice versa. The public key is publicly transmitted to the sender and used to encipher data that only the recipient can decipher. RSA is based on generating two large prime numbers, say P and Q and its security is enforced by the fact that albeit the fact that the product of these two primes $n = P \times Q$ is published, it is of enormous difficulty to factorize n.

A semiprime or (2 almost prime) or (pq number) is a natural number that is a product of 2 primes not necessary distinct. The semiprime is either a square of prime or square free. Also the square of any prime number is a semiprime number.

Mathematicians have been interested in many aspects of the semiprime numbers. In [5] authors derive a probabilistic function $g(y)$ for a number y to be semiprime and an asymptotic formula for counting $g(y)$ when y is very large. In [6] authors are interested in factorizing semiprimes and use an approximation to $\pi(n)$ the function that counts the prime numbers $\leq n$.

While mathematicians have achieved many important results concerning distribution of prime numbers, many are interested in semiprime properties as to counting prime and semiprime numbers not exceeding a given number.

From [7, 8, 9], the formula for $\pi^{(2)}(N)$ that counts the semiprime numbers not exceeding N is given by (1).

$$\pi^{(2)}(N) = \sum_{i=1}^{\pi(\sqrt{N})} \left[\pi\left(\frac{x}{p_i}\right) - i + 1 \right] \tag{1}$$

This formula is based on the primes P_1, P_2, … $P_{\pi(\sqrt{N})} \leq \sqrt{N}$.

Our contribution is of several folds. First, we present a formula to test the semiprimality of a given integer, this formula is used to build a new function $\pi^{(2)}(N)$ that counts the semiprimes not exceeding a given integer N using only $P_1, P_2, \ldots . P_{\pi(\sqrt[3]{N})} \leq \sqrt[3]{N}$. Second, we present an explicit formula that identifies the n^{th} semiprime number. And finally we give a formula that finds the next semiprime to any given number.

II. SEMIPRIMALITY TEST

With the same complexity $O(\sqrt{x})$ as the Sieve of Eratosthenes to test a primality of a given number x, we employ the Euclidean Algorithm and the fact that every prime number greater than 3 has the form $6k \pm 1$ and without previous knowledge about any prime, we can test the primality of $x \geq 8$ using the following procedure:

Define the following functions

$$T_0(x) = \left\lfloor \frac{1}{2}\left(\left\lceil \frac{x}{2} - \left\lfloor \frac{x}{2} \right\rfloor \right\rceil + \left\lceil \frac{x}{3} - \left\lfloor \frac{x}{3} \right\rfloor \right\rceil \right) \right\rfloor \quad (2)$$

$$T_1(x) = \left\lfloor \frac{1}{\left\lceil \frac{\sqrt{x}}{6} \right\rceil} \sum_{k=1}^{\left\lceil \frac{\sqrt{x}}{6} \right\rceil} \left\lceil \frac{x}{6k-1} - \left\lfloor \frac{x}{6k-1} \right\rfloor \right\rceil \right\rfloor \quad (3)$$

$$T_2(x) = \left\lfloor \frac{1}{\left\lceil \frac{\sqrt{x}}{6} \right\rceil} \sum_{k=1}^{\left\lceil \frac{\sqrt{x}}{6} \right\rceil} \left\lceil \frac{x}{6k+1} - \left\lfloor \frac{x}{6k+1} \right\rfloor \right\rceil \right\rfloor \quad (4)$$

$$T(x) = \left\lfloor \frac{T_0 + T_1 + T_2}{3} \right\rfloor \quad (5)$$

Where $\lfloor x \rfloor$ and $\lceil x \rceil$ are the floor and the ceiling functions of the real number x respectively.

We have the following theorem which is analog to that appeared in [10] with slight modification and the details of the proof are exactly the same.

Theorem 1: Given any positive integer $x > 7$, then

1. x is prime if and only if $T(x) = 1$
2. x is composite if and only if $T(x) = 0$
3. For $x > 7$

$$\pi(x) = 4 + \sum_{j=1}^{\left\lceil \frac{x-7}{6} \right\rceil} T(6j+7) + \sum_{j=1}^{\left\lceil \frac{x-5}{6} \right\rceil} T(6j+5) \quad (6)$$

counts the number of primes not exceeding x.

Now we proof the following Lemma:

Lemma 1: If N is a positive integer with at least 3 factors, then there exists a prime p such that:

$p \leq \sqrt[3]{N}$ and p divides N

Proof. If N has at least 3 factors then it can be represented as: $N = a.b.c$ with the assumption $1 < a \leq b \leq c$, we deduce that $N \geq a^3$ or $a \leq \sqrt[3]{N}$.

By the fundamental theorem of arithmetic, $\exists$ a prime number p such that p divides a. That means $p \leq a \leq \sqrt[3]{N}$, but p divides a and a divides N, hence p divides N with the property $p \leq \sqrt[3]{N}$.

Lemma 1: tells that, if N is not divisible by any prime $p \leq \sqrt[3]{N}$, then N has at most 2 prime factors, i.e., N is prime or semiprime . Using the proposed primality test defined by $T(x)$ we construct the semiprimality test as follows:

For $x \geq 8$, define the functions $K_1(x)$ and $K_2(x)$ as follows:

$$K_1(x) = \left\lfloor \frac{1}{\pi(\lfloor \sqrt[3]{x} \rfloor)} \sum_{i=1}^{\pi(\lfloor \sqrt[3]{x} \rfloor)} \left\lceil \left\lceil \frac{x}{p_i} \right\rceil - \frac{x}{p_i} \right\rceil \right\rfloor \quad (7)$$

$$K_2(x) = \left\lceil \frac{1}{\pi(\lfloor \sqrt[3]{x} \rfloor)} \sum_{i=1}^{\pi(\lfloor \sqrt[3]{x} \rfloor)} \left\lfloor \frac{x}{p_i} - \left\lceil \frac{x}{p_i} \right\rceil + 1 \right\rfloor T\left(\frac{x}{p_i} \right) \right\rceil \quad (8)$$

Where $\pi(x)$ is the classical prime counting function presented in (6), $T(x)$ is the same as in Theorem 1. Obviously $T(x)$ is independent of any previous knowledge of the prime numbers.

Lemma 2: If $K_1(x) = 0$, then x is divisible by some prime $p_i \leq \sqrt[3]{x}$.

Proof. For $K_1(x) = 0$, we have $\left\lceil \left\lceil \frac{x}{p_i} \right\rceil - \frac{x}{p_i} \right\rceil = 0$ for some p_i, then x is divisible by p_i for some $p_i \leq \sqrt[3]{x}$.

Lemma 3: If $K_1(x) = 1$,then x has at most 2 prime factors exceeding $\sqrt[3]{x}$.

Proof. If $K_1(x) = 1$, then $\left\lceil \left\lceil \frac{x}{p_i} \right\rceil - \frac{x}{p_i} \right\rceil = 1$ for all $p_i \leq \sqrt[3]{x}$ therefore by Lemma 1: , x is not divisible by any prime $p_i \leq \sqrt[3]{x}$, therefore x has at most two prime factors exceeding $\sqrt[3]{x}$.

Lemma 4: If $T(x) = 0$ and $K_1(x) = 1$, then x is semiprime and $K_2(x) = 0$.

Proof. If $K_1(x) = 1$, then x has at most 2 prime factors but $T(x) = 0$ which means that x is composite, hence x has exactly two prime factors and both factors are greater than

$\sqrt[3]{x}$ and $\left\lfloor \frac{x}{p_i} - \left\lceil \frac{x}{p_i} \right\rceil + 1 \right\rfloor = 0$ for each prime $p_i \le \sqrt[3]{x}$, therefore $K_2(x) = 0$.

Lemma 5: If $T(x) = 0$ and $K_1(x) = 0$, then x is a semiprime number if and only if $K_2(x) = 1$.

```
function [K1, K2] = k1_k2_of_x(x)
%-----------------------------------------------------
% This function receives x and returns k1 and k2
%    according to equations 7 and 8 in the paper.
%-----------------------------------------------------
    % Get the number and the list of primes <= x^(1/3)
    [r, Pr] = Pi_save(floor(nthroot(x, 3)));
    %  Compute K1(x) and K2(x)
    K1 = 0;
    K2 = 0;
    for i=1:r
        t1 = x/Pr(i);
        t2 = ceil(t1);
        t3 = T(t2,2);
        K1 = K1  + ceil(t2-t1);
        K2 = K2 + floor(t1 - t2 + 1)*t3;
    end
    K1 = floor(K1/r);
    K2 = ceil(K2/r);
end
```

Figure 1: MATLAB code for the computation of K_1 and K_2

Proof. If $T(x) = 0$ and $K_1(x) = 0$ then x divides a prime $p \le \sqrt[3]{N}$, but x is semiprime that means $x = pq$ and q is prime number hence for prime $p_i = p$ and $x = pq$ we have:

$$\left\lfloor \frac{x}{p_i} - \left\lceil \frac{x}{p_i} \right\rceil + 1 \right\rfloor T\left(\left\lceil \frac{x}{p_i} \right\rceil\right) = \left\lfloor \frac{pq}{p} - \left\lceil \frac{pq}{p} \right\rceil + 1 \right\rfloor T\left(\left\lceil \frac{pq}{p} \right\rceil\right) = 1$$

Consequently, $K_2(x) = 1$ because at least one of the terms is not zero.

Conversely, if $K_2(x) = 1$ then $\left\lfloor \frac{x}{p_i} - \left\lceil \frac{x}{p_i} \right\rceil + 1 \right\rfloor T\left(\left\lceil \frac{x}{p_i} \right\rceil\right)$ is not zero for some i and then $x = p_i q$ and $T\left(\left\lceil \frac{x}{p_i} \right\rceil\right) = 1$ for some prime $p_i \le \sqrt[3]{x}$ then $T\left(\left\lceil \frac{p_i q}{p_i} \right\rceil\right) = T(q) = 1$ hence q is a prime number and x is a semiprime number.

Figure 1 shows the MATLAB code for the computation of K_1 and K_2.

We are now in a position to prove the following theorem that characterizes the semiprime numbers.

Theorem 2: (Semiprimality Test): Given any positive integer $x > 7$, then x is semiprime if and only if:

1. $T(x) = 0$ and $K_1(x) = 1$

   or

2. $T(x) = 0$, $K_1(x) = 0$ and $K_2(x) = 1$

Proof. If x is semiprime, then $x = pq$ where p and q are two primes. If p and q both are greater than $\sqrt[3]{x}$ then $T(x) = 0$ and

$$K_1(pq) = \left\lfloor \frac{1}{\pi\left(\left\lfloor \sqrt[3]{pq} \right\rfloor\right)} \sum_{i=1}^{\pi\left(\left\lfloor \sqrt[3]{pq} \right\rfloor\right)} \left\lceil \left\lceil \frac{pq}{p_i} \right\rceil - \frac{pq}{p_i} \right\rceil \right\rfloor = \left\lfloor \frac{\pi\left(\left\lfloor \sqrt[3]{pq} \right\rfloor\right)}{\pi\left(\left\lfloor \sqrt[3]{pq} \right\rfloor\right)} \right\rfloor = 1$$

if $x = p'q'$ where p' and q' are two primes such that $p' \le \left\lfloor \sqrt[3]{x} \right\rfloor$ and $q' > \left\lfloor \sqrt[3]{x} \right\rfloor$ then $T(x) = 0$ and

$$K_1(p'q') = \left\lfloor \frac{1}{\pi\left(\left\lfloor \sqrt[3]{p'q'} \right\rfloor\right)} \sum_{i=1}^{\pi\left(\left\lfloor \sqrt[3]{p'q'} \right\rfloor\right)} \left\lceil \left\lceil \frac{p'q'}{p'} \right\rceil - \frac{p'q'}{p'} \right\rceil \right\rfloor = 0$$

because $\left\lceil \left\lceil \frac{p'q'}{p'} \right\rceil - \frac{p'q'}{p'} \right\rceil = 0$ and

$$K_2(p'q') = \left\lfloor \frac{1}{\pi\left(\left\lfloor \sqrt[3]{p'q'} \right\rfloor\right)} \sum_{i=1}^{\pi\left(\left\lfloor \sqrt[3]{p'q'} \right\rfloor\right)} \left\lfloor \frac{p'q'}{p'} - \left\lceil \frac{p'q'}{p'} \right\rceil + 1 \right\rfloor T\left(\frac{p'q'}{p'}\right) \right\rceil = 1$$

because $\left\lfloor \frac{p'q'}{p'} - \left\lceil \frac{p'q'}{p'} \right\rceil + 1 \right\rfloor T\left(\frac{p'q'}{p'}\right) = \lfloor q' - q' + 1 \rfloor T(q') = 1.$

The converse can be proved by the same arguments.

Corollary 1 A positive integer $x > 7$ is semiprime if and only if $K_1(x) + K_2(x) - T(x) = 1$.

Proof. A direct consequence of the previous theorem and lemmas.

III. Semiprime Counting Function

Notice that the triple $(T(x), K_1(x), K_2(x))$ have only the following 4 possible cases only:

Case 1. $(T(x), K_1(x), K_2(x)) = (1,1,0)$ indicates that x is prime number.

Case 2. $(T(x), K_1(x), K_2(x)) = (0,1,0)$ indicates that x is semiprime in the form $x = pq$ where p and q are primes that $\left\lfloor \sqrt[3]{x} \right\rfloor < p \le \left\lfloor \sqrt[2]{x} \right\rfloor$ and $q \ge \left\lfloor \sqrt[2]{x} \right\rfloor$.

Case 3. $(T(x), K_1(x), K_2(x)) = (0,0,1)$ indicates that x is semiprime in the form $x = pq$ where p and q are primes such that $p \le \left\lfloor \sqrt[3]{x} \right\rfloor$ and $q = \frac{x}{p} \ge \frac{x}{\sqrt[3]{x}} \ge \left\lfloor \sqrt[3]{x^2} \right\rfloor$.

Case 4. $(T(x), K_1(x), K_2(x)) = (0,0,0)$ indicates that x has at least 3 prime factors .

Using the previous observations, lemmas as well as Theorem 2: and corollary, we prove the following theorem that includes a function that counts all semiprimes not exceeding a given number N .

Theorem 3: For $N \ge 8$ then,

$$\pi^{(2)}(N) = 2 + \sum_{x=8}^{N} (K_1(x) + K_2(x) - T(x)) \qquad (9)$$

is a function that counts all semiprimes not exceeding N .

Figure 2 shows the MATLAB code for π^2 2 computation.

```
function [PI2 ] = pi2( x )
%
%  Count the number of semiprimes <= x
%
    PI2 = 2;
    for i=8:x
        [K1, K2] = k1_k2_of_x(i);
        PI2 = PI2 + K1 + K2 - T(i,2);
    end
end
```

Figure 2: MATLAB code for π^2

IV. N^{th} SEMIPRIME FORMULA

The first few semiprimes in ascending order are $sp_1 = 4$, $sp_2 = 6$, $sp_3 = 9$, $sp_4 = 10$, $sp_5 = 14$, $sp_6 = 15$, $sp_7 = 21$, etc.

We define the function $G(n,x) = \left\lfloor \frac{2n}{n+x+1} \right\rfloor$ where $n = 1,2,3...$ and $x = 0,1,2,3...$

clearly

$$G(n,x) = \left\lfloor \frac{2n}{n+x+1} \right\rfloor = \begin{cases} 1 & x < n \\ 0 & x \ge n \end{cases}$$

Knowing that the bound of the n^{th} prime is $P_n \le 2n\log n$ [11], we can say that the n^{th} semiprime $sp_n \le 2$ $P_n \le 4n\log n$.

Theorem 4: For $x \ge 8$ and $n > 2$, sp_n the n^{th} semiprime is given by the formula:

$$sp_n = 8 + \sum_{x=8}^{\lfloor 4n\ln n \rfloor} \left\lfloor \frac{2n}{n+1+\pi^{(2)}(x)} \right\rfloor = 8 + \sum_{x=8}^{\lfloor 4n\ln n \rfloor} \left\lfloor \frac{2n}{n+3+\sum_{m=8}^{x}(K_1(m)+K_2(m)-T(m))} \right\rfloor$$

The formula in full is given by:

$$sp_n = 8 + \sum_{x=8}^{\lfloor 4n\ln n \rfloor} \left\lfloor \frac{2n}{n+3+\sum_{m=8}^{x}\left(\left\lfloor \frac{1}{\pi(\lfloor\sqrt[3]{m}\rfloor)} \sum_{i=1}^{\pi(\lfloor\sqrt[3]{m}\rfloor)} \left\lceil \left\lceil \frac{m}{p_i} \right\rceil - \frac{m}{p_i} \right\rceil \right\rfloor + \left\lceil \frac{1}{\pi(\lfloor\sqrt[3]{m}\rfloor)} \sum_{i=1}^{\pi(\lfloor\sqrt[3]{m}\rfloor)} \left\lfloor \frac{m}{p_i} - \left\lceil \frac{m}{p_i} \right\rceil + 1 \right\rfloor T\left(\frac{m}{p_i}\right) \right\rceil - T(m)\right)} \right\rfloor$$

where $T(m)$ is given by

$$T(m) = \left\lfloor \frac{T_0(m)+T_1(m)+T_2(m)}{3} \right\rfloor$$

$$= \left\lfloor \frac{1}{3}\left(\left\lfloor \frac{1}{2}\left(\left\lceil \frac{m}{2} - \left\lfloor \frac{m}{2} \right\rfloor \right\rceil + \left\lceil \frac{m}{3} - \left\lfloor \frac{m}{3} \right\rfloor \right\rceil \right) \right\rfloor + \left\lfloor \frac{1}{\left\lceil \frac{\sqrt{m}}{6} \% \right\rceil} \sum_{k=1}^{\left\lceil \frac{\sqrt{m}}{6} \right\rceil} \left\lceil \frac{m}{6k-1} - \left\lfloor \frac{m}{6k-1} \right\rfloor \right\rceil \right\rfloor + \left\lfloor \frac{1}{\left\lceil \frac{\sqrt{m}}{6} \right\rceil} \sum_{k=1}^{\left\lceil \frac{\sqrt{m}}{6} \right\rceil} \left\lceil \frac{m}{6k+1} - \left\lfloor \frac{m}{6k+1} \right\rfloor \right\rceil \right\rfloor \right) \right\rfloor$$

Proof. For the n^{th} semiprime sp_n , $\pi^{(2)}(sp_n) = n$ and for $x < sp_i$, $pi^{(2)}(x) < pi^{(2)}(sp_i) = i \ \forall\, i = 1,2,3,....,n$.

Using the properties of the function

$$G(n,x) = \left\lfloor \frac{2n}{n+x+1} \right\rfloor = \begin{cases} 1 & x < n \\ 0 & x \ge n \end{cases}$$

we compute

$$8 + \sum_{x=8}^{\lfloor 4n\ln \rfloor} \left\lfloor \frac{2n}{\%n+1+\pi^{(2)}(x)} \right\rfloor = 8 + \sum_{x=8}^{\lfloor 4n\ln \rfloor} G(n, \pi^{(2)}(x))$$
$$= 8 + G(n,\pi^{(2)}(8)) + G(n,\pi^{(2)}(9))$$
$$+ G(n,\pi^{(2)}(10)) + ... + G(n,\pi^{(2)}(P_{n-1})) + ...$$
$$+ G(n,\pi^{(2)}(P_{n-1}+1))$$
$$+ ....G(n,\pi^{(2)}(P_n)) + G(n,\pi^{(2)}(P_n+1)) + ...$$
$$= 8+1+1+1+...1+0+0+0+... = sp_n$$

where the last 1 in the summation is the value of $G(n,\pi^{(2)}(sp_{n-1}))$ and then followed by $G(n,\pi^{(2)}(sp_n)) = G(n,n) = 0$ followed by zeroes for the rest terms of the summation, hence

$$sp_n = 8 + \sum_{x=8}^{\lfloor 4n\ln n \rfloor} G(n, \pi^2(x)) = 8 + \sum_{x=8}^{\lfloor 4n\ln n \rfloor} \left\lfloor \frac{2n}{n+1+\pi^{(2)}(x)} \right\rfloor$$

As an example, computing the 5^{th} semiprime number gives $sp_5 = 8+1+1+1+1+1+1+1 = 14$ as shown in Table 1.

$\pi^2(8)=2$	$G(5,\pi^2(8))=1$
$\pi^2(9)=3$	$G(5,\pi^2(9))=1$
$\pi^2(10)=4$	$G(5,\pi^2(10))=1$
$\pi^2(11)=4$	$G(5,\pi^2(11))=1$
$\pi^2(12)=4$	$G(5,\pi^2(12))=1$
$\pi^2(13)=4$	$G(5,\pi^2(13))=1$
$\pi^2(14)=5$	$G(5,\pi^2(14))=0$

Table 1: Computing the 5^{th} semiprime

Figure 3 shows the MATLAB code for the n^{th} semiprime computation.

```
function [nth ] = nth_semiprime( n )
    %
    %  Gives the nth semiprime for n>2
    %
    nth = 8;
    minb = 8;
    maxb = floor(4*n*log(n));
    num = 2*n;
    for i=minb:maxb
        [PI2 ] = a2_pi2_kbased( i );
        denom = n+1+PI2;
        fra = floor(num/denom);
        nth = nth + fra;
        if (fra == 0)
            break;
        end
    end
end
```

Figure 3: MATLAB code for sp_n

V. NEXT SEMIPRIME

In our previous work [10], we introduced a formula that finds the next prime to a given number. In this section, we use an enhancement formula to find the next prime to a given number and we introduce a formula to compute the next semiprime to any given number.

Recall that the integer $x \geq 8$ is a semiprime number if and only if $K_1(x)+K_2(x)-T(x)=1$ and if x is not semiprime then $K_1(x)+K_2(x)-T(x)=0$.

Now we introduce an algorithm that computes the next semiprime to any given positive integer N.

Theorem 5: If N is any positive integer greater than 8 then the next semiprime to N is given by:

$$NextSP(N) = N+1+\sum_{i=1}^{N}\left(\prod_{x=N+1}^{x=N+i}\left(1+T(x)-K_1(x)-K_2(x)\right)\right) \quad (10)$$

where $T(x), K_1(x), K_2(x)$ are the functions defined in Section 2.

Proof. We compute the summation:

$$\sum_{i=1}^{N}\left(\prod_{x=N+1}^{x=N+i}(1+T(x)-K_1(x)-K_2(x))\right)$$

$$= \sum_{i=1}^{NextSP(N)-N-1}\left(\prod_{x=N+1}^{x=N+i}(1+T(x)-K_1(x)-K_2(x))\right)+$$

$$\sum_{i=NextSP(N)-N}^{N}\left(\prod_{x=N+1}^{x=N+i}(1+T(x)-K_1(x)-K_2(x))\right)$$

$$= \sum_{i=1}^{NextP(N)-N-1}(1) + \sum_{i=NextP(N)-N}^{N}(0)$$

$$= NextSP(N)-N-1$$

hense

$$NextSP(N) = N+1+\sum_{i=1}^{N}\left(\prod_{x=N+1}^{x=N+i}(1+T(x)-K_1(x)-K_2(x))\right)$$

x	$\pi^2(x)$	Time in seconds
10	4	0.00
100	34	0.01
1000	299	0.1
10000	2625	3.0
100000	23378	50
1000000	210035	1091
10000000	1904324	22333
100000000	17427258	508840

Table 2: Testing on $\pi^{(2)}(x)$

VI. RESULTS

We implemented the proposed functions using MATLAB and complete the testing on an Intel Core i7-6700K with 8M cache and a clock speed of 4.0GHz. Table 2 shows the results related to $\pi^2(x)$ for some selected values of x.

We have also computed few n^{th} semiprimes as shown in Table 3.

n	sp_n	Time in seconds
100	314	0.07
200	669	0.24
300	1003	0.49
400	1355	0.86
500	1735	1.22
600	2098	1.89
700	2474	2.39
800	2866	3.40
900	3202	3.78
1000	3595	4.91
5000	19643	105.72
10000	40882	579.01

Table 3: Testing on n^{th} semiprimes

And finally we show the next semiprimes to some selected integers in Table 4.

n	$NextSP(n)$	Time in seconds
100	106	0.01
200	201	0.02
300	301	0.04
400	403	0.07
500	501	0.09
1000	1003	0.31
5000	5001	5.92
10000	10001	22.38

Table 4: Testing on $NextSP(n)$ semiprimes

VII. CONCLUSION

In this work, we presented new formulas for semiprimes. First, $\pi^{(2)}(n)$ that counts the number of semiprimes not exceeding a given number n. Our proposed formula requires knowing only the primes that are less or equal $\sqrt[3]{n}$ while existing formulas require at least knowing the primes that are less or equal $\sqrt[2]{n}$. We also present a new formula to identify the n^{th} semiprime and finally, a new formula that gives the next semiprime to any integer.

REFERENCES

[1] "Standard specifications for public key cryptography (p1363)," pp. 367–389, 1998. [Online]. Available: http://grouper.ieee.org/groups/1363/

[2] E. Rescorla, SSL and TLS: designing and building secure systems. Addison-Wesley Reading, 2001, vol. 1.

[3] J. Clark and P. C. van Oorschot, "Sok: Ssl and https: Revisiting past challenges and evaluating certificate trust model enhancements," in Security and Privacy (SP), 2013 IEEE Symposium on. IEEE, 2013, pp. 511–525.

[4] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120–126, 1978.

[5] S. Ishmukhametov and F. F. Sharifullina, "On a distrubution of semiprime numbers," Izvestiya Vysshikh Uchebnykh Zavedenii. Matematika, no. 8, pp. 53–59, 2014.

[6] R. Doss, "An approximation for euler phi," Northcentral University Prescott Valley, United States o, 2013.

[7] E. W. Weisstein, "Semiprime," Wolfram Research, Inc., 2003.

[8] J. H. Conway, H. Dietrich, and E. A. Brien, "Counting groups: gnus, moas and other exotica," Math. Intelligencer, vol. 30, no. 2, pp. 6–15, 2008.

[9] D. A. Goldston, S. Graham, J. Pintz, and C. Y. Yildirim, "Small gaps between primes or almost primes," Transactions of the American Mathematical Society, pp. 5285–5330, 2009.

[10] I. Kaddoura and S. Abdul-Nabi, "On formula to compute primes and the nth prime," Applied Mathematical Sciences, vol. 6, no. 76, pp. 3751–3757, 2012.

[11] G. Robin, "Estimation de la fonction de tchebychef Θ sur le k-ième nombre premier et grandes valeurs de la fonction w(n) nombre de diviseurs premiers de n," Acta Arithmetica, vol. 42, no. 4, pp. 367–389, 1983.