ISSN: 2663-5798 || Arab Journal for Scientific Publishing

الإصدار السابع – العدد ثمانية وستون
تاريخ الإصدار: 2 – حزيران – 2024م
www.ajsp.net

"Modular Square One-Way Function & Square Root Algorithm"

(Analyzing the algorithm for randomness, regularity schematic (codec system) and vector normalization)

Researcher:

Ahmed Mohammed Al-Fahdi

Sultanate Of Oman

MSc communication engineering

University of Birmingham

ISSN: 2663-5798 || Arab Journal for Scientific Publishing

الإصدار السابع – العدد ثمانية وستون
تاريخ الإصدار: 2 – حزيران – 2024م
www.ajsp.net

Abstract:

Actually, The proposed paper was built as one part working through analyzing one-way modular square which is a special case of modular exponentiation with exponent of 2, counter form of quadratic residue, for encryption and PKI implementation. Later on, Due to the amount of data regarding this analysis, it seems be better to separate it to three parts. This paper (Part-1) aims to analyze a modular square one-way function using integer factorization (IF) or approximation methods. It is supposed that such function has random characteristics. This analysis considers a new innovative idea, original as claimed, focusing in notable regularities that could be used as a trapdoor for practical applications. Such as random generator, new codec system and 3D vector normalization. At the end, different types of quadratic residue algorithms and square root will be considered.

Key words: Square root algorithm, Modular square, Modular arithmetic, Quadratic nonresidue square root, One-way function, Newton-Raphson method, Exponentiation by squaring, Jacobi prime, Legendre symbol, Fast inverse square root (Invsqrt), Vector normalization.

1. Introduction

Since the far past square roots was fascinating task and this was utilitarian by the area computations. Through over centuries studies in such roots add a lot to the arithmetic science. These days, it is realized that not every natural number is a perfect square. Such square roots are nonintegral and even irrational. As squaring an integer is number result from multiplying the integer by itself. In the other hand, the square root of an integer could result in irrational number. Approximating such number to an integer result in a remainder. Such reminder is called modular square or quadratic residue or nonresidue. In addition to all that, calculating a square root of large numbers it will be tedious using integer factorization (IF). In such case there is a need of square root algorithm. This algorithm exploits the underlying algebra of the decimal place of the floating value. [1] [2]

$$y = f(x) = x^2 \pmod{n} \quad (1)$$

Usually the modular square function (1) characterize a randomness. It is type of modular arithmetic where integers wrap around when reaching certain value called modulus. Such arithmetic is similar to 12-hour clock, in which the day is divided into two 12-hour periods. In general, according to studies and modular graphs of arithmetic function, the modular for multiplication look more diverse than addition. As a special case the modular of the modular exponent the modular square look even more random and have no apparent symmetry. It is surprised that the modular graphs for higher powers look more regular again. [3]

2. Methodology and paper organization

2.1 Overview

The overall paper take analyzing the one-way square modular algorithm for encryption and PKI implementation. Due to the amount of data and type of the information we decide to divide the whole content to three parts. First part (PART-1), analyze the square modular function in term of arithmetic modular using integer factorization and Newton Raphson approximation. Such mathematics allow us to analyze the function in term of randomness. Also, it will allow us to figure out if there is any regularity schematic that could be exploit as new codec system! In addition, exploring the practical implementation of the square modular and fast inverse square root algorithm allow to implement it in vector normalization. [4][5]

2.2 Modular Square function

In mathematics, there are only few functions assumed (conjectured) to be one-way. None of these functions is proven to be one-way. It is theoretically not even known the proof of existence of such functions. Modular square function (1) is supposed to be a one-way function. It is also called square function. [1]

$$y = f(x) = x^2 \ (mod\ n)$$

analyzing the nonresidue quadratic root, for non-perfect squares, of this function using techniques such as integer factorization (IF), discrete logarithmic (DL) and quadratic nonresidue (QR) leads to focus in the integer factorization (IF) as simple start point. As a result of quadratic nonresidue Integers, the resulting arithmetic modular supposed to be irrational number, for noncomplete squares. For such calculation, in this methodology, a way of numerical analysis will be used called Newton's approximation method which is also known as Newton-Raphson method. This way will help to find the roots or zeros with a real-valued function f and its derivative f'.For illustration, in geometrically respective this allow to approximate the zeros using tangent of the function graph (Figure-1). The execution of a linear approximation is in repeated process with a recursive partitioning procedure. [6]

ISSN: 2663-5798 || Arab Journal for Scientific Publishing
الإصدار السابع – العدد ثمانية وستون
تاريخ الإصدار: 2 – حزيران – 2024م
www.ajsp.net

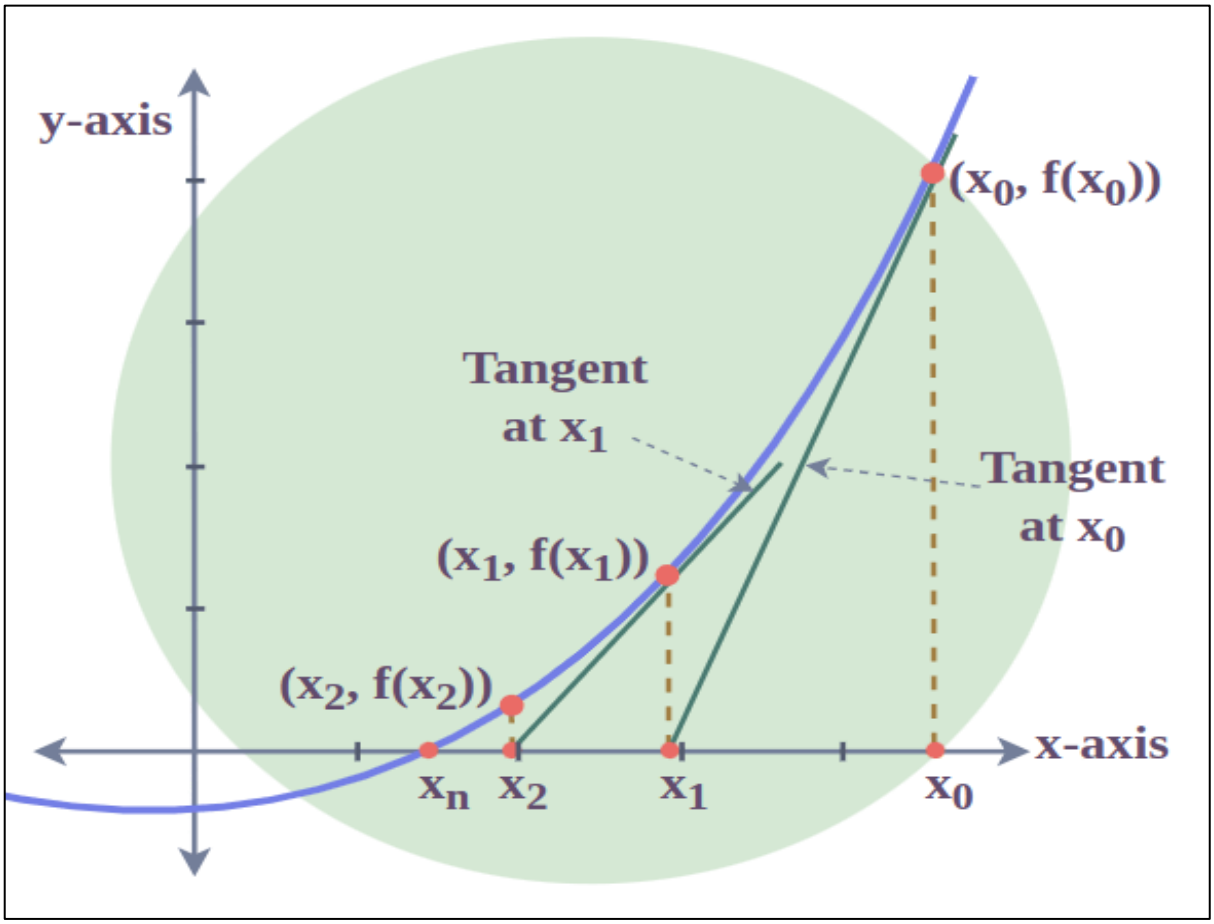


Figure (1): Newton Raphson approximation illustration as intersect of the tangent /geeksforgeeks.org/newton-raphson-method/

2.3 Mathematics

The mathematic for Newton-Raphson approximation is as follow

$$X_{i+1} = X_n - \frac{f(x_i)}{f'(x_i)} \quad (2)$$

So, for modular square function

$f(x_i) = x^2 - x_i$ (3)

$f'^{(x_i)} = 2x$ (4)

Such calculation will be done manually till a sufficiently precise value is reached. This will allow us to approximate the root as well with the modular or remainder. [10]

Later on, we could do such calculations using the calculator and proceed with the following procedure for the remainder of the squares to analyze such values. Other parameters could be calculated for deeper view of numerical theory analysis with such function.

From above, the square root of non-perfect square is irrational number. Hence, the integer part could be approximated to the nearest integer using the usual way of threshold (0.5).

Furthermore, approximating the rational part, rational decimal, needs to evaluate thresholds using (1-3) functions as follow:

$$x_{i+1} = x_n - \frac{f(x_i)}{f'(x_i)}$$

Where

$$f(x_i) = x^2 - x_i$$

$$f'(x_i) = 2x$$

Approximating x_1 from x_0 leads to

$$x_1 = x_0 - \frac{x^2 - x_0}{2x}$$

But in this Newton iteration

$x^2 \approx x_0^2$ & $x \approx x_0$

So,,,

$$x_1 = x_0 - \frac{x_0^2 - x_0}{2x_0}$$

$$x_1 = x_0 - \frac{x_0 - 1}{2}$$

$$x_1 = \frac{x_0 + 1}{2} \qquad (5)$$

But for rational decimals $-1 \leq x_0 \leq 1$

So

$$x_1 = \begin{cases} 0 & for \ x_0 = -1 \\ \frac{1}{2} & for \ x_0 = 0 \\ 1 & for \ x_0 = 1 \end{cases} \qquad (6)$$

This means that the resulting rational decimal calculated from the approximation process need to be approximated to the nearest value as what doing with the integers. For quadratic nonresidue irrational number, there are infinite rational numbers of the rational part between 0 and 1. These irrational parts follow a gaussian distribution with mean value 0.5, because it is the only exact finite number in this scale, or either sides 0 and 1 using threshold of 0.25 or 0.75. This could be illustrated in figure (2)

ISSN: 2663-5798 || Arab Journal for Scientific Publishing

الإصدار السابع – العدد ثمانية وستون
تاريخ الإصدار: 2 – حزيران – 2024م
www.ajsp.net

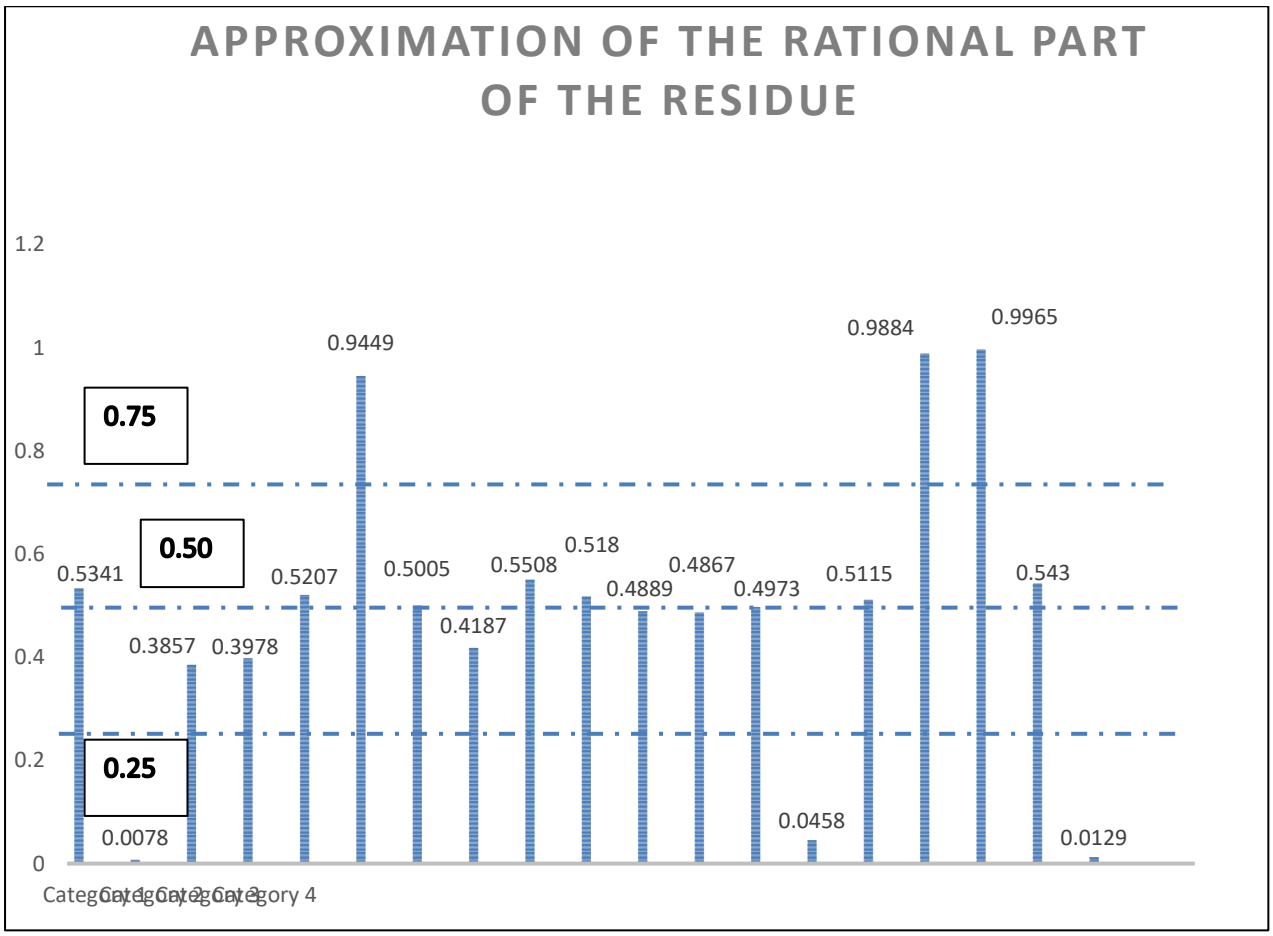


Figure (2): rational part approximation

Notice-1: The Methodology trick used here is that from above functions it is easy to calculate the square modular (r) approximated to the closest integer using rational part approximation with threshold of 0.5. The same thing is done with the rational part of the root modular (n) approximated to the ratio of 0.5 using threshold of ¼ and ¾.

3. Results

The following table summarize the calculations that have been done in the above section resulting from equations (1-6) where:

x^2:is the square, non-perfect squares chosed randomly

x: is the square root

r: is the square remainder approximated to integer $(x^2 - x_{app}^2)$

n :is the ratio, from rational par, of the root remainder

$$(x_{exact} - x_{app}) \times x_{app}$$

$\frac{n}{r}$: is the notified correlation between n and r

ISSN: 2663-5798 || Arab Journal for Scientific Publishing

الإصدار السابع – العدد ثمانية وستون
تاريخ الإصدار: 2 – حزيران – 2024م

www.ajsp.net

Num	x^2	x_{app}	r	Exact n	approx n	$\frac{n}{r}$
1	612	25	-13	6.5341	6.5	-0.5
2	570	24	-6	3.0078	3	-0.5
3	811	28	27	13.3857	13.5	0.5
4	550	23	21	10.3978	10.5	0.5
5	1011	32	-13	6.5207	6.5	-0.5
6	1111	33	22	10.9449	11	0.5
7	2022	45	-3	1.5005	1.5	-0.5
8	41	6	5	2.4187	2.5	0.5
9	59	8	-5	2.5508	2.5	-0.5
10	61	8	-3	1.5180	1.5	-0.5
11	103	10	3	1.4889	1.5	0.5
12	2131	46	27	7.4867	13.5	0.5
13	2311	48	15	3.4973	7.5	0.5
14	2777	53	7	16.0458	3.5	0.5
15	3119	56	-17	8.5115	8.5	-0.5
16	2130	46	14	6.9884	7	0.5
17	2312	48	-8	3.9965	4	-0.5
18	2778	53	-31	15.5430	15.5	-0.5
19	3118	56	-18	9.0129	9	-0.5

Table (1): Summarizing results of the Methodology section

Notice-2: From number analysis, it is clear that the square number residue (r) could be directly extracted as double of the root modular ratio (n) without the traditional subtraction method.

After the suggested approximations, the ratio of the root modular to the square modular has fixed magnitude of (0.5) with alternating sign as shown in the below figure (3).

ISSN: 2663-5798 || Arab Journal for Scientific Publishing
الإصدار السابع – العدد ثمانية وستون
تاريخ الإصدار: 2 – حزيران – 2024م
www.ajsp.net

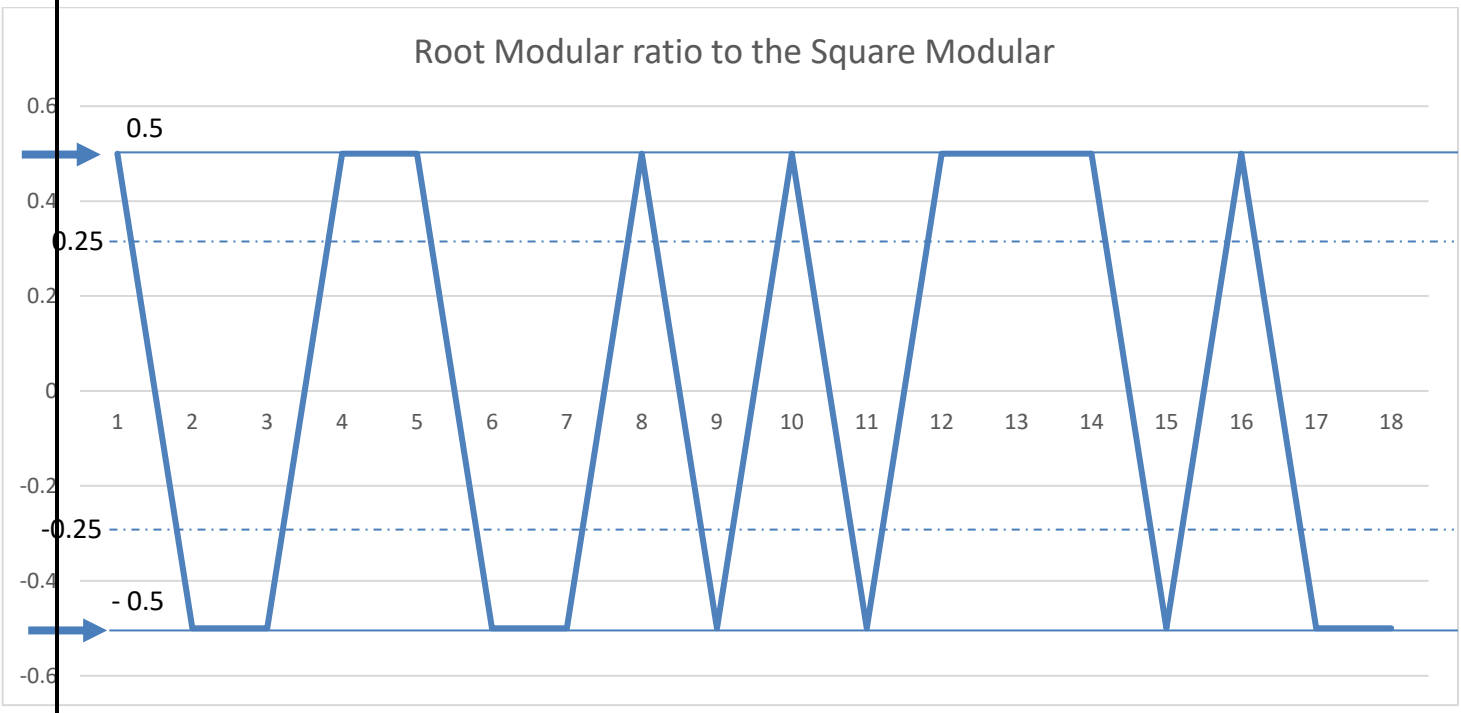


Figure (3): Root Modular ratio to the Square Modular with fixed magnitude at (0.5)

4. Results Analyzing:

Form above methodology and results a case study has been considered above for modular square one-way function using equation (7):

$$r = x^2 - x_{app}^2 \qquad (7)$$

Analyzing the relation of such residue to the ratio of the rational part of the root using equation (8):

$$n = (x - x_{app}) \times x_{app} \qquad (8)$$

Going through the methodology above with the explained trick by calculating the residue of the rational root itself approximated to ½ ratio using thresholds of ¾ and ¼. Such characteristic could be examined in another paper. It is clear that:

$$r = 2 \times n \qquad (9)$$

or

$$n = \frac{r}{2} \qquad (10)$$

Where:

- r: is the modular square relative to the square of the approximated root
- n: is the rational ratio of the modular root relative to the approximated root
- Notice: It is clear that n work as a trapdoor for easy calculation of the remainder r.

ISSN: 2663-5798 || Arab Journal for Scientific Publishing

الإصدار السابع – العدد ثمانية وستون
تاريخ الإصدار: 2 – حزيران – 2024م
www.ajsp.net

For the results and functions analyzed above and referring to the Legendre symbol that is used for the quadratic residue as a quadratic character modulo of an odd prime number. In somehow, the quadratic residue function (11) is similar to the modular square function (1) which is a special case of the modular exponent function as follow:

Quadratic residue function

$$x^2 = q(mod\ n) \qquad (11)$$

Modular square function

$$q = x^2\ (mod\ n) \qquad (1)$$

$$Legendre\left(\frac{a}{b}\right) = \begin{cases} -1 & quadratic\ residue\ modulo\ p \\ 0 & a \equiv 0(mod\ p) \\ 1 & quadratic\ nonresidue\ modulo\ p \end{cases} \qquad (12)$$

That is, in the methodology above, the modular square function (1) has been studied for the approximated integer root so that:

$$r = x^2\ (mod\ x_{app})$$

Inspired by the Legendre symbol (12) and Jacobi symbol with the notified iteration of $(\frac{n}{r})$ in table (1), it is helpful to represent the ratio of the rational root modular to the square modular $(\frac{n}{r})$ by a normalized symbol, lets represent it as modular factor (M), with values of -1,0 and 1 as follow:

$$M\left(\frac{n}{r}\right) = \begin{cases} -1 & for\frac{n}{r} = -0.5 \\ 0 & for\frac{n}{r} = 0 \\ 1 & for\frac{n}{r} = 0.5 \end{cases} \qquad (13)$$

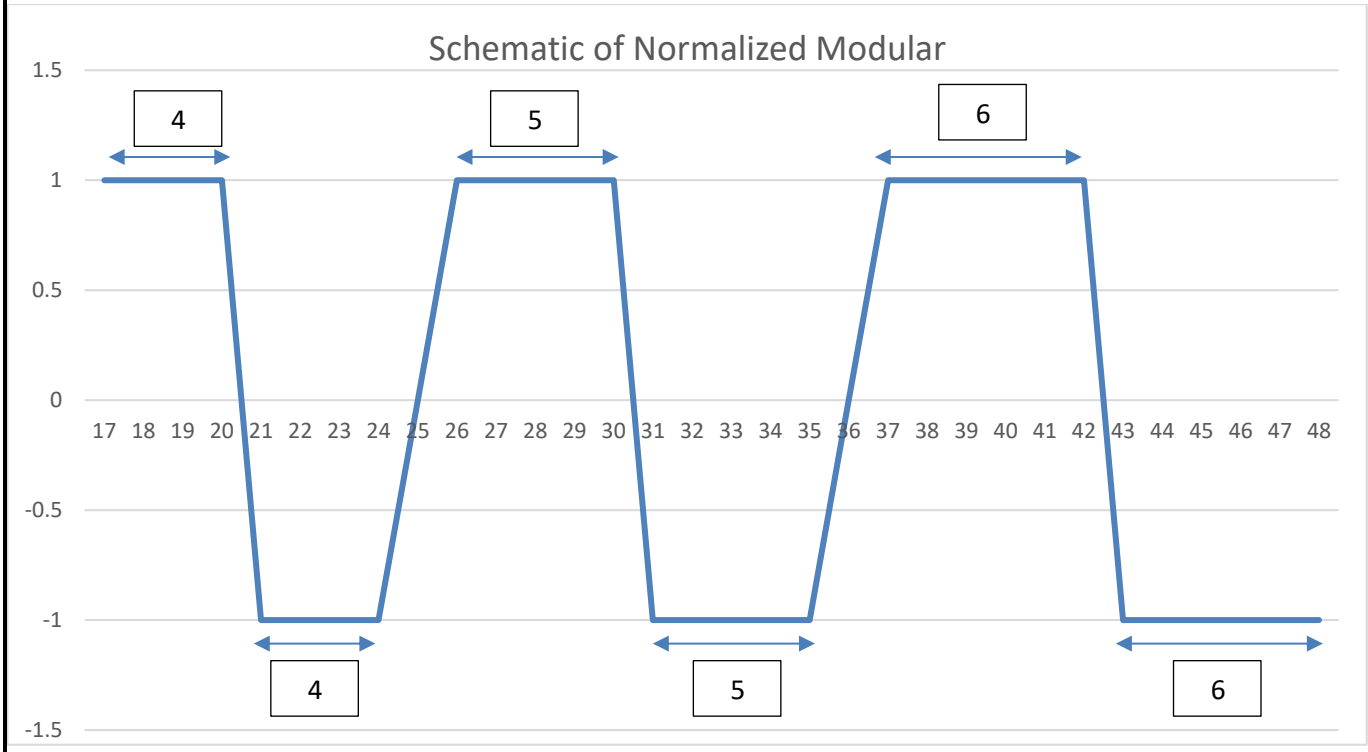
As a result, this symbol could be examined for squares scale, chosen randomly [17-48] in the table (2) below

	Integers (x^2)	r	n	M (normalized residue)
	17	1	0.5	1
	18	2	1	1
	19	3	1.5	1
	20	4	2	1
	21	-4	2	-1
	22	-3	1.5	-1
	23	-2	1	-1
	24	-1	.5	-1
	25	0	0	0
	26	1	.5	1
	27	2	1	1
	28	3	1.5	1
	29	4	2	1
	30	5	2.5	1
	31	-5	2.5	-1
	32	-4	2	-1

	33	-3	1.5	-1
	34	-2	1	-1
	35	-1	.5	-1
	36	0	0	0
	37	1	.5	1
	38	2	1	1
	39	3	1.5	1
	40	4	2	1
	41	5	2.5	1
	42	6	3	1
	43	6	3	-1
	44	5	2.5	-1
	45	4	2	-1
	46	3	1.5	-1
	47	2	1	-1
	48	1	.5	-1

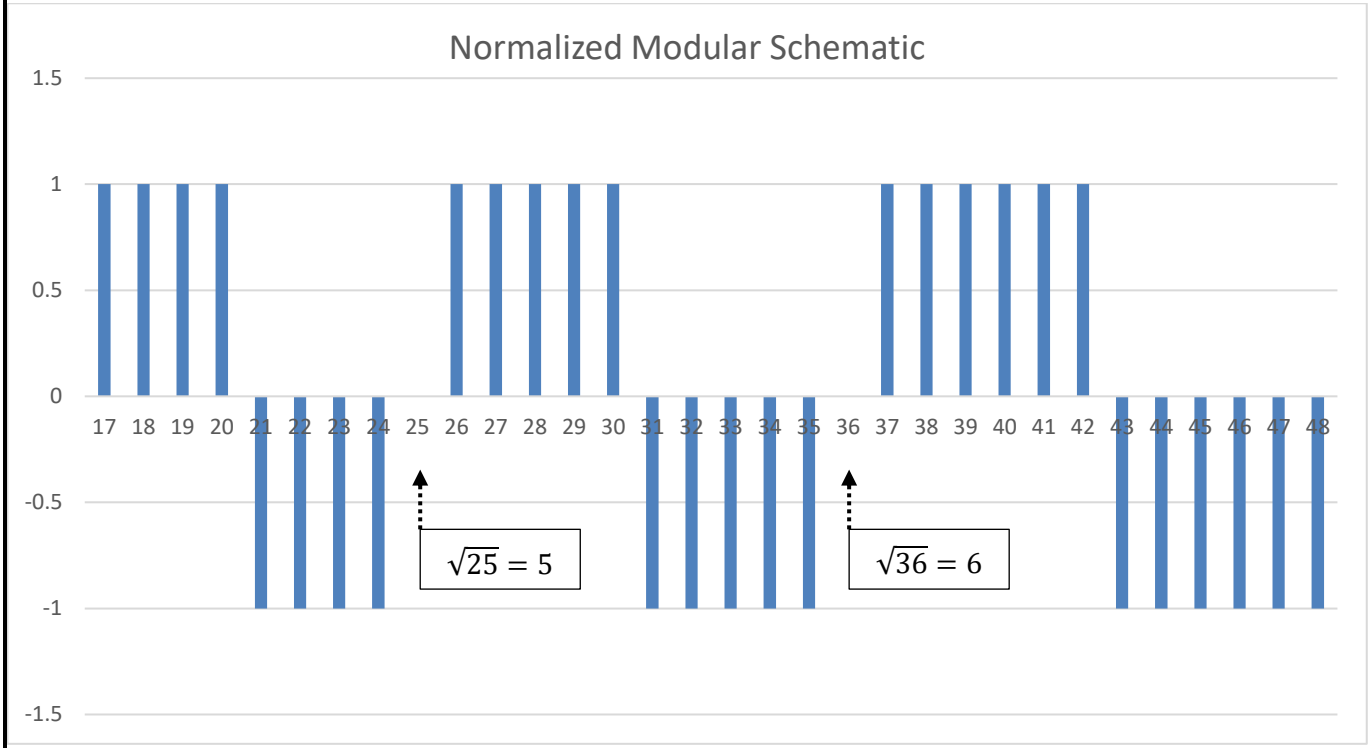
Table (2): Normalized modular ratio (Symbol M)

From the table (2) above, although the known randomness property of the square modular function, there is a striking regularity represented by the normalized modular factor(M).Such regularity could be illustrated by plotting graphs (figure 4-5) below



Figure(4):Line chart of the normalized modular factor (M) - equation (13)

ISSN: 2663-5798 || Arab Journal for Scientific Publishing
الإصدار السابع – العدد ثمانية وستون
تاريخ الإصدار: 2 – حزيران – 2024م
www.ajsp.net



Figure(5):Column chart of the normalized modular factor (M) - equation (13)

From figure (4) above, it is notified that the pulse width is equal to the root of the lowest complete square. In addition to that, the symbol of normalizing the ratio of the square modular to the rational root modular could be simplified by the follow definition:

$$M = \begin{cases} 1 & for\ square\ approximation\ lower\ complete\ square \\ 0 & for\ any\ complete\ square \\ -1 & for\ square\ approximation\ above\ complete\ square \end{cases}$$

Analyzing figure (5), warped around any complete square there are equal a count of positive and negative symbols equal to the root of that complete square.

Notice: Implementing the methodology trick to exponent higher than square, 3 ,4,5 does not work, need further examine. That means such ($\frac{r}{n}$) trapdoor does not work with the exponential modular one-way algorithm higher than 2 as further it has been trayed. This enhances that the modular square function as a special case of the modular exponent function.

5. Implementation and practical applications:

Although it seems that the analysis of the above algorithm done in the results analyzing section (4) simple and direct, it is applicable for many applications such as codec, cryptography and 3D graphic games. These are high tech fields in term of signal processing.

According to the results analyzing (part4) and the previous background in signal processing, the analyzed characteristics of the studied algorithm is useful for the following fields:

a- Randomness System applications:

a.1 Although the randomness of the square modular, it is notable that there is a striking regularity for the ratio of the rational root modular to the square modular and this regularity schematic increase for the higher perfect squares as shown in figure (5). This in turn, represent that the perfect squares space away for higher values. Considering the prime-counting function $\pi(n)$ shown in the figure (6), It is supersizing to figure out that there is a direct relationship related to the growth rate of (M). This is something related to the prime number theorem. Furthermore, the prime number density (equation-14), has normal or gaussian probability which in turn reflected to the rational part of the irrational roots and hence the modular factor (M) around any perfect root shown in figure (5). [8]*

$$\lim_{x\to\infty} \frac{\pi(x)}{x/log\ (x)} = 1 \quad (14)$$

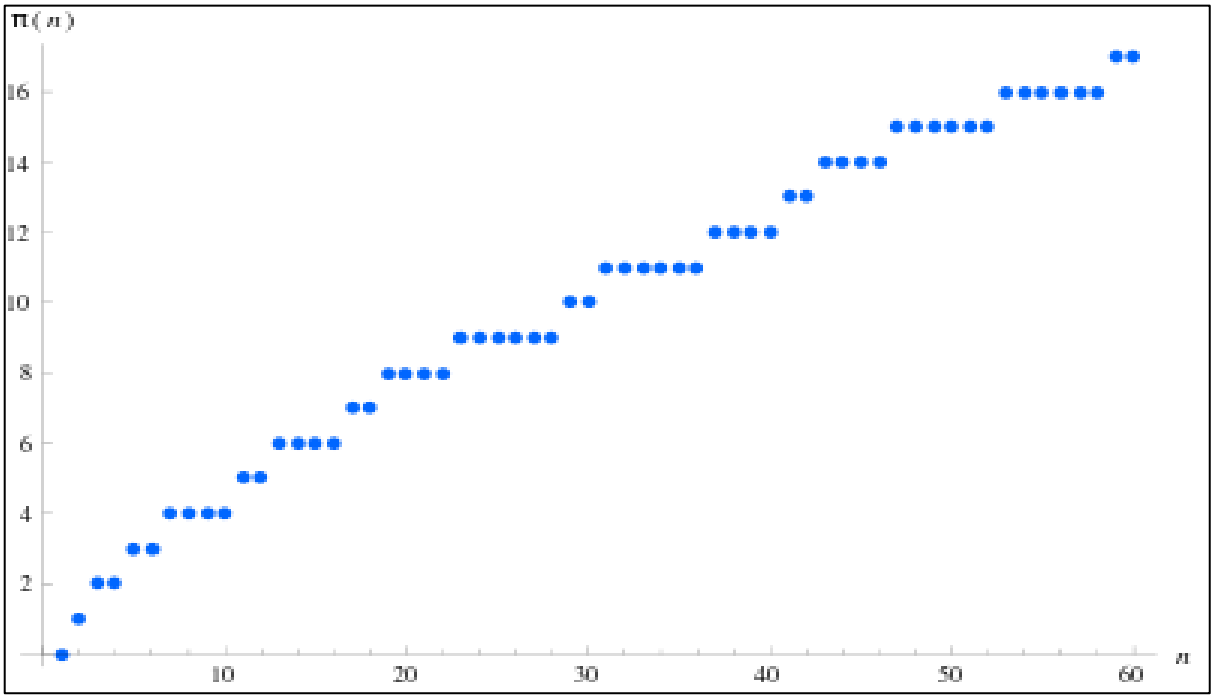


Figure (6): Values of $\pi(n)$ for the first 60 positive integers [8]

b- Codec System applications:

b.1 As shown above, the prime number density function $\pi(n)$ follow similar characteristic to the density of modular factor (M). Furthermore, it is known that from prime number theorem such function follows Gaussian probability and it is applied to what is called Multi-Dimensional Gaussian classifier and Multivariate normal distribution. This is an advantage for audio and video CODEC

b.2 According to the above characteristics and the characteristic of alternating sign with the Modular factor M , such algorithm could be used as practical application for Hilbert envelop transform with special case of the Riemann-Hilbert problem. [8]

b.3 Considering the figure (6), there is window schematic algorithm with scalable interval and zeros at perfect squares. Such Windows with gaussian characteristic is applicable for filters to remove the airy disks caused by diffraction. This window with zero skewness at the perfect squares could be used also for smoothing the signal in similar way to Hann function.

b.4 Using such codec for compression it is assumed to be lossless compression which allows the data for further processing including encryption or hashing.

b.5 Such regularity characteristics applied for PCM from analogue to digital modulation such as that with a-law and μ-law with manipulated property of sampling rate and the bit depth to represent each sample. In such coding the complete square could be synchronized to Nyquist frequency or (or folding frequency). Such characteristic allows to have free of aliasing distortion samples. This could be clarified by transferring the time-based algorithm to frequency based using Laplace transformation. [9]

C- Vector Normalizing applications:

Vector normalizing is done by scaling the vector to the magnitude such that:

$V = ax + by + cz$ (15)

Magnitude =$|V| = \sqrt[2]{a^2 + b^2 + c^2}$

Then normalized vector $v = \frac{V}{|V|} = \frac{ax+by+cz}{\sqrt[2]{a^2+b^2+c^2}}$

That means multiplying the vector by the inverse square root ($\frac{1}{\sqrt[2]{a^2+b^2+c^2}}$)

As a result of above, the square root algorithm in inverse form is used for vector normalization. There is a c-code algorithm (Appendix [1]) called Fast Inverse Square Root algorithm referred as Fast InvSqrt (). It depends in the bit-fiddling techniques followed by Newton iterations, as it has been done above in the methodology section. It was used by 3dfx Interactive. In 2005, it become famous algorithm in the world of games as it is used by Id Software. This is because it was mysterious algorithm for the programmers as it depends on bits hacking playing with the rational part decimal, something similar to what have been done above in the methodology. The magic of such popularity was with the Magic number ($0x5F3759DF$) that use to minimize the approximation error and not known precisely how it was determined. It was derived through trial and error.

Because of its speed the algorithm was used in graphics of video games to normalize the surface for lightening and shading calculations. Such algorithm can work as a hint to use the above result analysis for vector normalization. [10]

6. Conclusion

In conclusion, throughout this paper one-way modular square function was analyzed. This function is a special case of modular exponentiation, which built the infrastructure of public-key cryptography. Square root function was first milestone in such analyzation. Integer factorization method was used throughout Newton Raphson approximation method. Although such method is not practical for computer science in term of speed, it was easy practical way for modular manual calculations analysis. From such analysis a normalized residue symbol M, similar Legendre, was proposed as a trapdoor for the square modular calculation. By trial and error, such trapdoor does not work with higher modular exponentiation. The characteristics shown by M propose different practical applications in cryptography, codec systems and vectors normalization.

Newton approximation method is avoided in computer science as it contains slow division operation. In contrast to that, for computation purposes, fast inverse square root was analyzed. Such method depends on a bit fiddling technique by shifting

rational part decimal followed by Newton iteration. There are many other algorithms could be used for square modular such as Tonelli-Shanks and Cipolla's algorithms. They were for quadratic residue (equation-11) similar to square modular (equation-1)

The square root function analysis may play pivotal role in future with quantum computations. This is applied for the quantum circuit gates and the quantum algorithms. This paper (part-1), presented as a foundation of other two papers (part-2 & part-3) dealing with cryptography and mathematical conjectures.

Appendix:

[1] Fast Inverse Square Root [10]

```
//Fast Inverse Square Root//


float Q_rsqrt(float number)
{
 long i;
 float x2, y;
 const float threehalfs = 1.5F;


 x2 = number * 0.5F;
 y  = number;
 i  = * ( long * ) &y;                  // evil floating point bit level hacking
 i  = 0x5f3759df - ( i >> 1 );          // what the fuck?
 y  = * ( float * ) &i;
 y  = y * ( threehalfs - ( x2 * y * y ) );   // 1st iteration
 // y  = y * ( threehalfs - ( x2 * y * y ) );   // 2nd iteration, this can be removed


 return y;
}
```

ISSN: 2663-5798 || Arab Journal for Scientific Publishing

الإصدار السابع – العدد ثمانية وستون
تاريخ الإصدار: 2 – حزيران – 2024م
www.ajsp.net

Quote

“If you couldn’t can’t explain it simply, you don’t understand it well enough “Albert Einstein…

References:

Prof . Dr. Rolf Oppliger,Contemporary to Cryptography,Infogaurd,Bar Switzerland ,2013
W. Diffie and M. Hellman”New Direction in Cryptography”,IEEE Trans, 1976
Center for education in mathematics and computing, Grade 6 Math Circles -Modular Arithmetic,University of Waterloo,2020
Catalano,Fiore,Rosario,Vamvourellis,Algebraic (Trapdoor) One-Way Functions and their Applications, University of Catania
Evan Huynh,Rabin’s Cryptosystem, Department of Mathematics, Linnaeus University, Sweden 2021
Anca-Maria Nica ,Quadratic Residues and Applications in Cryptography, Alexandru Ioan Cuza Universithy of Iasi, 2020
Pranav Gokhale ,Implementation of Square Root Function Using Quantum Circuits, Princton University Class, 2015.
F.B. Roodenburg,Riemann’s Explicit Formula and the Prime Number Theorem, Delft Institute of Applied Mathmatics, 2020
Dushyant,Patrick,Nikolay, Non Intrusive Codec Identification Algorithm ,Marsh 2012
Andrei Seymour-Howell,Fast inverse square-root program,2021

"وظيفة مربعة نمطية في اتجاه واحد وخوارزمية الجذر التربيعي"

تحليل الخوارزمية من حيث العشوائية والتخطيط الانتظامي (نظام الترميز) وتطبيع المتجهات

إعداد الباحث:

احمد محمد الفهدي

سلطنة عمان

ماجستير هندسة الاتصالات

الملخص:

في الواقع، تم بناء البحث المقترح كجزء واحد يعمل على تحليل المربع المعياري أحادي الاتجاه وهو حالة خاصة من الأس المعياري ذو الأس 2، الشكل المضاد للبقايا التربيعية، للتشفير وتنفيذ البنية التحتية للمفاتيح العامة .(PKI) لاحقًا، نظرًا لكمية البيانات المتعلقة بهذا التحليل، يبدو من الأفضل تقسيمه إلى ثلاثة أجزاء. تهدف هذه الورقة (الجزء الأول) إلى تحليل دالة مربعة نمطية أحادية الاتجاه باستخدام تحليل الأعداد الصحيحة (IF) أو طرق التقريب. ومن المفترض أن هذه الوظيفة لها خصائص عشوائية. يتناول هذا التحليل فكرة مبتكرة جديدة، أصلية كما يُزعم، مع التركيز على الانتظامات الملحوظة التي يمكن استخدامها كباب سحري للتطبيقات العملية. مثل المولد العشوائي ونظام الترميز الجديد وتطبيع المتجهات ثلاثية الأبعاد. في النهاية، سيتم النظر في أنواع مختلفة من خوارزميات البقايا التربيعية والجذر التربيعي.

الكلمات المفتاحية: خوارزمية الجذر التربيعي، المربع المعياري، الحساب المعياري، الجذر التربيعي غير المتبقي، الدالة أحادية الاتجاه، طريقة نيوتن–رافسون، الأس بالتربيع، رئيس جاكوبي، رمز ليجيندر، الجذر التربيعي العكسي السريع(Invsqrt) ، تطبيع المتجهات.