International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 3 (2018) Spl.

Analysis of cryptographic Algorithms Based on Vedic Mathematics

Lisha A
Mary matha Arts & Science College
Kannur University
Mananthavady-670745, Wayanad
Kerala, India

Thomas Monoth
Mary matha Arts & Science College
Kannur University
Mananthavady-670645, Wayanad
Kerala, India

***Abstract*— Cryptography generally deals with encrypting and decrypting of message with large mathematical operations. Long mathematical calculations may be needed in most cases. This may consume much power, hardware and processing time. To get maximum security with the limited resources is the real challenge here. So we need smart algorithms. The ancient Rigvedic mathematics that was rediscovered by Bharathi Krishna Tirtaji contains many mathematical shortcuts that can be used to make such smart algorithms; this study is an analysis of researches done towards the development of cryptographic algorithms using vedic mathematics so far.**

Keywords*— Vedic Mathematics; Vedic Sutras; Cryptography; RSA; AES; ECC

I. INTRODUCTION

This paper is a review of various researches carried out to improvise computer algorithms using the vedic mathematics sutras with a special focus to cryptography. Cryptography is the technique for making the message secure. In cryptography encryption is the process of translation of data into a secret code. AES (Advance Encryption System), RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography) etc. are some standard encryption decryption algorithms.

This paper is organized is as, Section 2 describes the vedic mathematics and explanation of vedic sutras. Section 3 describes application of vedic mathematics in cryptography algorithms. Analysis of computational complexity of different algorithms using vedic mathematics presented in section 4 and conclusion offered in section 5.

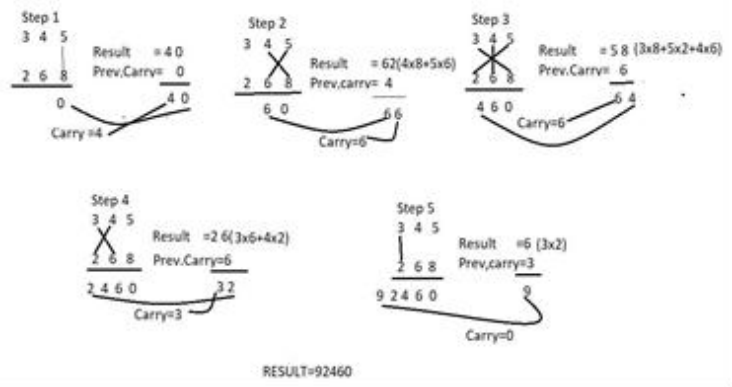
II. VEDIC SUTRAS

There are sixteen sutras and fifteen sub sutras in Rig-Veda according to Tirthaji and the detailed explanation of them is given in his book [1].The arithmetic operations addition, subtraction, multiplication and division can perform efficiently by the sixteen sutras. The sutras based on multiplication and division can be applied in many computer algorithms and many researches are carried out towards the usage of them.

Multiplication and division are the most important operation in cryptography algorithms. Reduced operation in multiplication and division will increases the speed of the algorithms. Urdhva-Tiryagbyham sutra,Nikhilam Navatashcaramam Dashatah sutra and Dhawajanka sutra in vedic mathematics are efficient for multiplication and division. These sutras are explained below:

A. Urdhva-Tiryagbyham Sutra for Multiplication

Urdhva tiryagbhyam sutra is the general shortcut applicable to all cases of multiplication and division of a large numbers. It literally means "Vertically and cross wise."
In fig 1, this method is explained with multiplication of two decimal numbers 345 and 268.



Initially the LSB digits on the both numbers of the line are multiplies and added with the carry from the previous step. This generates one of the bits of the result and carry. This carry is added in the next step and the process goes on likewise. When there are more lines in one step, all the results are added to previous carry.

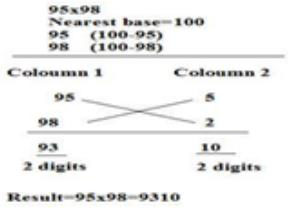
Since there is a parallel generation of the partial product and their sums, the processor becomes independent of the clock frequency. The advantage here is that parallelism reduces the need of the processor to operate at increasingly high clock frequency and this optimizes the processing power [2].

B. Nikhilam Sutra for Multiplication

Nikhilam Navatashcaramam Dashatah sutra means 'all from 9 and last from 10'. This sutra is suitable for multiplying large numbers. This method take the subtraction of a number from nearest power of 10.ie..10,100,1000 etc. It finds out the compliment of the large number from its nearest base to perform the multiplication operation on it, hence larger the original number, lesser the complexity of the multiplication. The procedure as follows:

Numbers are below base number.

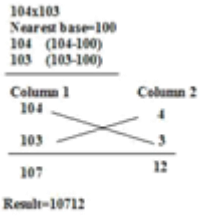
Consider the example 95x98 .Here 95 and 98 are below the base 100.



First the two numbers are subtracted from the base. We can write the numbers in two columns, one consisting of the numbers to be multiplied (Column 1) and other consisting of their complements (Column 2). The result will have two parts, RHS of the answer is the product of the deviations of the numbers ie.5x2=10. The left hand side(LHS) of the product can be found by cross subtracting the second number of Column 2 from the first number of Column 1 or vice versa, a, i.e., 95 -2=93 or 98 -5 = 93.The final result is obtained by concatenating RHS and LHS (Answer = 9310).

Numbers are above base number

Example: Consider 104x103. Here the multiplier and multiplicand are above the base 100.



Here the base is subtracted from the number and the result also have two parts, RHS of the answer is the product of the deviations of the numbers ie.4x3=12. The LHS of the product can be found by cross adding the second number of the column 2 with the first number of the column 1 or vise versa.ie.104+3=107 or 103+4=107. The final result is 10712.

This technique have only two multiplication steps and it is less complex [3].This techniques is applicable in all multiplication cases however it is more effective when higher order number are involved.

C. Nikhilam Sutra for Division

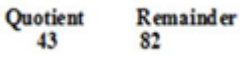
Nikhilam Navatashcaramam Dashatah sutra in Division is applied when divisor is closer to and slightly lesser than power of 10.

Example: 4382/99

Step1: Split dividend in two parts (quotient and remainder)in such a way remainder to have same digits as that of divisor. Here it is 2.

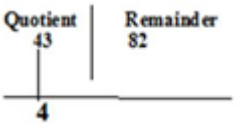
Dividend: 4382

Divisor: 99

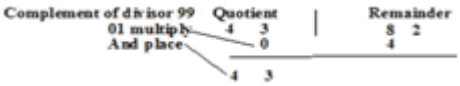


Step 2: Take complement of divisor 01 (100-99=01) .This is called deficiency.

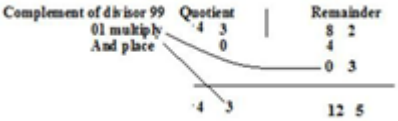
Step 3: Take first digit down as it is



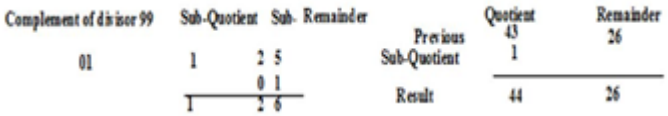
Step 4: Multiply the deficiency (01) with first digit (4), shift one place to right and then write below 3 and 8.Now add the first column.



Step 5: The above step repeated and add column wise till the number is filled in last column and then added column wise.



Step 6: In few cases it may be possible that remainder is greater than the divisor which is not possible. In this case divide the remainder with the divisor that results in subquotient and sub-remainder. Add sub-quotient with original quotient and sub-remainder becomes the final remainder.



Here we see that the division operation has been done with multiplication and addition operations. Multiplication is relatively faster and cheaper operation than division. This results in faster and less complex operation [4].

D. Dhawajanka Sutra for division

Dhawajanka Sutra is the upa sutra of vedic mathematics which means 'on the top of the flag', is a generalized formula for division. It is based on the formula Urdhva-tiryagbhyam. Steps of the division is performed in dhawajanka sutra is given below [5]

Step 1: The divisor and dividend are arranged in the form shown below. Only leftmost digit of divisor is left aside. Dividend is separated in two sections right part consisting number of digits equal to digits in divisor. Divisor is represented by d, dividend by X and quotient by A.

Step 2: Only first digit of dividend is divided by the left out digit, quotient and remainder of this division are noted.
Step 3: During next iteration remainder from previous iteration is used with next digit of dividend. Quotient digits and dividend digits without leftmost digit are multiplied in vertically and crosswise manner. This product is subtracted from number formed by combination of remainder and digit of remainder.
Step 4: Number left after subtraction in step 3 is divided by left out digit of divisor quotient is noted and remainder is prefixed with rest of the digits of dividend.
Step 5: This process is continued till same number of quotient digits equal to digits in left part of dividend is obtained.
Step 6: Remainder is obtained by subtraction of right part of dividend prefixed by last remainder and cross multiplication of quotient and divisor.
This sutra produces same results whether applied to large or small divisors.

III. Vedic Mathematics in Cryptographic Algorithms

Privacy and security has become an important feature with the growth of electronic communication. Cryptography is a technique for making the message secure. There are various cryptographic algorithms. In this analysis we use the most popular cryptographic algorithms such as AES (Advance Encryption System), RSA(Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography). RSA public key cryptosystem is a popular method in public key cryptography. For providing security in network RSA is the safest high quality standard algorithm. . AES is a symmetric encryption algorithm developed in 1998 by Joan Daemen and Vincent Rijmen. AES algorithm supports any combination of data and key length of 128,192 and 256 bits. ECC is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller and more efficient cryptographic keys.

R G Kaduskar [6] proposes a new architecture for RSA algorithm using vedic mathematics. The division algorithm of vedic mathematics, nikhilam and arunanka are used to create a new architecture for RSA algorithm. It is highly time consuming to implement modular exponentiation operations in very large integer numbers. The researcher proposes to use vedic mathematics for such operations in RSA algorithms. It was found more effective when Sutras were used for calculations and when compared with basic architecture implementation. R Bhaskar et al. [7] used vedic mathematics and improved restoring division algorithm to improve the computation speed of RSA encryption system. The sutra they have used is Urdhva – Tiryagbhyam which is a multiplication Vedic shortcut. The key generation consume considerable amount of time and hardware for encryption and decryption. The vedic multiplier increase the computation speed with minimized hardware.

Greeshma Liz Jose et al. [8] made a comparison of performance of vedic multiplication and division algorithms and the conventional algorithms based on speed, power and area. Then vedic algorithms are used to implement the RSA encryption and decryption system. The vedic RSA enabled the RSA hardware to work as fast as its software counterparts. R Thamil Chelvan et al. [9] proposes the implementation of RSA encryption/decryption algorithm using the Dhavajanka sutra in vedic mathematics for division operation. It is found that when implementing vedic division algorithm, the RSA circuitry has less timing delay compared to multipliers and division algorithms. It is also efficient in terms of area/speed.

The RSA algorithm lacks only in encryption speed because of its mathematical computation. To increase the speed the multiplier based on vedic mathematics is used. Also the hardware is quite complex. In order to make it compatible with digital hardware Dhanashri R Kadu et al.[10] used the urdhva Tiryakbhyam sutra in multiplication of binary number system instead of decimal number system. The objective of the work proposed by Shahina M. Salim [11] are to design and implement the RSA cryptosystem to improve speed performance, area reduction and throughput.

To improve performance they used vedic mathematics in key generation of RSA encryption and decryption algorithm. It is found that this design is efficient in terms of area and speed. Soumya Sadandan et al. [12] introduced area efficient design for performing various operations involved in AES method of cryptography. One of the crucial mathematical operations performed during AES is the mix column steps in AES. Computation of mix columns and its inverse is considered to be even more difficult task. Urdhava Tiryakbhyam sutra of vedic mathematics is used in proposed architecture for mix columns and its inverse. The architecture performs better when compared with conventional AES in terms of area. Shrita G et al. [13] have also proposed a novel method for the mix column and inverse mix columns operation in AES cryptography. They found that by implementing the proposed system is efficient in terms of speed and area. Kavuri Suresh et al. [14] in their paper proposed an architecture using vedic mathematics for performing mix and inverse mix column computation in AES. They achieved a 100% area efficiency and a two times increase in speed by the novel algorithm, in comparison with two other popular implementations of the same. Anjali L[15] in her paper presents a low area, cost effective AES cipher for encryption /decryption using a 128 bit iterative architecture. In this work, the amount of hardware resources has been optimized with respect to various proposed designs on alternative platforms.

Scalar multiplication in point addition and point doubling in ECC is the most time consuming process. Prokash Barman et al. [16] used vedic sutra for scalar multiplication. By comparing the conventional multipliers they found that the functional speed of ECC arithmetic increased by using vedic multiplier. Shylashree.N, D et al. [17] proposed a high speed ECC using vedic mathematics. They found that proposed

vedic multiplication is six times faster than the other methods previously used when applied in point doubling

IV. ANALYSIS OF COMPUTATIONAL COMPLEXITY OF ALGORITHMS BASED ON VEDIC MATHEMATICS

To evaluate the performance of vedic mathematics algorithms researchers recommended various parameters such as time, delay, power and number of slices. Here we analysed computational complexity of algorithms using vedic mathematics proposed by different researchers are given in table 1.

Table1. Performance Analysis of vedic Algorithms

Sl No	Author/Title of the paper	Name of cryptographic Algorithm used	Computational Complexity
1	R G Kaduskar et.al[6]	RSA	Efficient in Time
2	Bhaskar R et.al [7]		Improve computation speed& efficient in hardware
3	Greeshma Liz Jose et.al. [8]		Efficient in Terms of speed and Area
4	Kadu R Dhanashri [9]		Reduce complexity, execution time, power etc.
5	Thamil Chelvan R et.al.[10]		Efficient in time, speed and area
6	Shahina M. Salim et.al.[11]		Efficient in time and area
7	Soumya Sadanandan et.al. [12]	AES	Effiecient in performance and use less area
8	Shrita G et al.[13]		Area efficient and high speed
9	Suresh Kavuri et al.[14]		Perform well in terms of speed and occupies less area
10	Anjali.L[15]		Efficient in terms of area and hardware resources
11	Prokash Barman et al.[16]	ECC	Increase speed of arithmetic in ECC
12	Shylashree.N, D et al. [17]		Increase Speed of scalar multiplication.

By the analysis from the table we see that by using vedic sutras the algorithms are efficient in time, area and power.

V. CONCLUSION

In this paper, we analyzed various researches carried out to use vedic sutras in computer algorithms with a special focus to the cryptographic algorithms such as RSA, AES and ECC, All the researchers recommend the use of vedic shortcuts in algorithms to save hardware resources and processing time. In future these shortcuts can be applied for other cryptographic algorithms such as DES. The increase in speed could also allow Cryptographers to use larger key sizes for greater security.

References

[1] Jagadguru Swami Sri Bharath, Krsna Tirathji Maharaja, "Vedic Mathematic or Sixteen Simple Mathematical Formulae from veda", Motilal Banarsidas , Varanasi(India,1965). J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.

[2] M.Valli , Dr.A.R.Pon Periasamy, "Design of high speed Vedic Multiplier Using K-Map Boolean Function Techniques", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4(5), 2016.pp.8141-8148 .

[3] Manoranjan Pradhan, Rutuparna Panda and Sushanta Kumar Sahu, "Speed Comparison of 16x16 Vedic Multipliers", International Journal of Computer Applications ,Vol 21(6), 2011.

[4] Diganta Sengupta, Mahamuda Sultana, Atal Chaudhuri, "Vedivision– A Fast BCD Division Algorithm Facilitated By Vedic Mathematics", International Journal of Computer Science & Information Technology (IJCSIT, Vol 5(4), August 2013.

[5] Anchaliya Ruchi.,Chiranjeevi G .N., and Subhas Kulkarni, "Efficient Computing Technique using Vedic Mathematics Sutra", International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering 3(5), pp. 24-27.

[6] R G Kaduskar , "A New Architecture for RSA Algorithm using Vedic Mathematics", 2011 Fourth International Conference on Emerging Trends in Engineering & Technology , pp.233-237.

[7] R Bhaskar, Ganapathi Hegde and P R Vaya, "An Efficient Model for RSA Encryption System Using Vedic Mathematics ", International Conference on Communication Technology and System Design 2011, pp.124-128.

[8] Greeshma Liz Jose, Sani John., "VLSI Implentation of Vedic Mathematics and Its Application in RSA Cryptosystem", IJIRD Vol 2(10),October 2013.

[9] R Thamil Chelvan, S Roobini Priya, "Implementation of Fixed and Floating Point Division using Dhavajanka Sutra", International Journal of VLSI and Embedded Systems-IJVES, Vol 4(2),March-April 2013

[10] Dhanashri R Kadu and Dr.G P Dhok.,"A Novel Efficient Technique For Data Security using Vedic Mathematics", International Journal of Application or Innovation In Engineering & Managemant(IJAIEM), Vol 4(5),May 2015.

[11] Shahina M. Salim, Sonal A. Lakhotiya.," Implementation of RSA Cryptosystem Using Ancient Indian Vedic mathematics", International Journal of Science and Research (IJSR), Volume 4 (5), May 2015, pp-3221-3230.

[12] Soumya Sadanandan, Anjali," Design of advanced encryption standard using Vedic Mathematics", International Journal of Innovative Research in Advanced Engineering(IJIRAE) Vol 1 (6), July 2014.

[13] Shrita G and Basavaraj S M, "A Novel Architecture for Inverse Mix Operation in AES using Vedic Mathematics", International Journal of engineering & Research technology January 2015.

[14] Kavuri Suresh and Jagadish Reddy," Implementation of AES algorithm using Urdhwa Tiryakbhyam Sutra and Galois field", International Journals and Magazine of Engineering, Technology, Management and Research, Volumn 2 (7) July 2015 pp. 1545-1550.

[15] Anjali.L ," An Efficient Hardware FPGA Implementation of AES-128 Cryptosystem Using Vedic Multiplier and Non LFSR", International Journal of Scientific Research Engineering & Technology (IJSRET), Volume 3(5), August 2014.pp.842-846

[16] Prokash Barman, Banani Saha,"An Efficient Elliptic curve Cryptography Arithmetic Using Nikilam Multiplication".,The International Journal of Engineering and Science. Vol4(4). Pp.45-50,2015.

[17] Shylashree.N, D. Venkata Narayana Reddy and V. Sridhar," Efficient Implementation of Scalar Multiplication for Elliptic Curve Cryptography using Ancient Indian Vedic Mathematics over GF (p)", International Journal of Computer Applications Volume 49(7), July 2012.pp.46-50 .