ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 3, Issue 5, May 2015

Efficient Computing Techniques using Vedic Mathematics Sutras

Ruchi Anchaliya[1], Chiranjeevi G.N.[2], Subhash Kulkarni[3]

M.Tech Student (VLSI & Embedded Systems- 4th Sem), Department. of ECE, PESIT South Campus, Bangalore, India[1]

Assistant Professor, Department of ECE, PESIT South Campus, Bangalore, India[2]

HOD, Department of ECE, PESIT South Campus, Bangalore, India[3]

Abstract: This paper describes various Vedic Mathematics Sutras for arithmetic calculations. Vedic Mathematics is the ancient methodology of Indian mathematics which has a unique computational technique for calculations based on 16 Sutras (Formulae). Application of the Sutras saves a lot of time and effort in solving the problems as compared to formal methods. This paper describes Dwandwayoga Sutra for Square, Urdhva Tiryakbhyam Sutra for multiplication, Dhwajanka Sutra for division. The coding is done in Verilog HDL and the FPGA synthesis is done using Xilinx Spartan library. The results show that total delay in computation is reduced by using Vedic Mathematics.

Keywords: Dwandwayoga Sutra, Urdhva Tiryakbhyam Sutra, Dhwajanka sutra, Nikhilam sutra, Arunanka sutra, Vedic Mathematics, Cryptography.

I. INTRODUCTION

Today's world is dependent on e-mail, secure telephony, mobile internet, e-commerce, e-banking and soon. So, it's necessary to secure the data transmitted over the network. Cryptographic systems provide information security: confidentiality, authentication, data integrity and non-repudiation. Cryptography is the study of methods for sending messages in secret so that only the intended recipient can read the message. Data is encrypted by the sender and after transmission decrypted at the receiver end to get the original data.

RSA (Rivest, Shamir, Adleman) and ECC are the safest standard algorithms, based on public-key, for providing security in networks.

One of the most time consuming operation in RSA is modular exponentiation operation on large integers (computation of $a^b \bmod n$ where a is the text, (b,n) is the key) which can be improved by Vedic Mathematics Sutras. Using Vedic Sutra for division, quotient and remainder can be calculated much quickly as compared to normal division. But the key size in RSA is large so ECC is preferred over RSA as key size for encryption is small in ECC. For ECC algorithm, time taken to perform point multiplication can be reduced by implementing successive point doubling and point addition in Vedic Mathematics, to make ECC algorithm more efficient.

The performance of most crypto systems is primarily determined by an efficient implementation of arithmetic operations. Vedic sutras provide efficient methods for these computations thereby increasing the efficiency of cryptographic systems. Different algorithms for network key security have been studied and various vedic mathematics sutras have been analysed which can improve the efficiency of security algorithm. Since the performance of any algorithm depends on the efficient arithmetic operations, if time taken to perform these arithmetic operations is reduced, performance can be improved a lot.

II. REVIEW WORK

R.Thamil Chelvan and S.Roobini Priya have proposed a division technique which is based on modification of addition circuitry [1]. This reference paper is about the implementation of RSA encryption/ decryption algorithm using the algorithms of Ancient Indian Vedic mathematics that has been modified to improve performance in Xilinx platform. The project shows that RSA circuitry implemented using Vedic division is efficient in terms of area and speed, compared to its implementation using conventional division architecture. For the Xilinx Spartan family, it is found that the gate delay for RSA circuitry has been highly improved by using Vedic Mathematics. The hardware implementation of the Rivest- Shamir-Adleman (RSA) algorithm is presented by Mr. R.G.Kaduskar [2]. The architecture is specifically based on the sutras named 'Nikhilam' and 'Arunanka'. He proposed a division algorithm based on Vedic sutras 'Nikhilam'and 'Arunanka' to compute the modular exponentiation in the Encryption block. The basic architecture for RSA algorithm has been modified by addition of certain blocks like, Linear Feedback Shift Register, Private Key Generator etc. Also, instead of using memory section, the architecture is redefined with the use of modular exponentiation algorithm and modular multiplication algorithm. The most significant aspect of this paper is the development of an architecture based on the Ancient Indian Vedic Mathematics.

ECC is another public key cryptographic system. The main feature of ECC is that it relies on the difficulty of solving ECDLP (Elliptic Curve Discrete Log Problem) in the same way as RSA depends on the difficulty of factoring the product of two large primes. The best known

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526
INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 3, Issue 5, May 2015

method for solving ECDLP is fully exponential, whereas the number field sieve (for factoring) is sub-exponential. This allows ECC to use drastically smaller keys to provide equivalent security.

Kuldeep Bhardwaj and Sanjay Chaudhary described ECC which offers more security with per bit increase in key size than other existing public key techniques [3]. So that, due to much smaller key sizes involved, ECC provides faster implementation. This reference paper shows the processes of implementation of operations on elliptic curves using 'C' language. It has been observed that ECC is better than other public key cryptographic systems as it uses small key size. Elliptic curve cryptography is widely used in many areas because of its small key size. It is used in devices which have less storage memory. ECC is most popularly used in Smart cards. Smart cards are being used as bank (credit/debit) cards, electronic tickets and personal identification (or registration) cards.

Ankita Soni and Nisheeth Saxena described the idea of ECC and application of elliptic curve in cryptography [4]. It illustrates the process of encryption and decryption of a message by transforming the message into an affine point on the Elliptic curve. A comparison is performed between the encrypted text messages using different key sizes to calculate the time consumed by each. This reference paper showed that ECC uses small key size which results in faster execution time.

III. VEDIC MATHEMATICS

A. Square using Dwandwayoga Sutra

For squaring, a dedicated architecture can improve its performance than using multiplier architecture. Using Duplex D property of binary numbers from the sutra Dwandwayoga of Vedic Mathematics algorithm for squaring is implemented.

1) Duplex of a number is twice that number, Duplex of a is a^2
2) Duplex of two numbers is multiplying two with the product of that number, Duplex of ab is 2*a*b
3) Duplex of three numbers is multiplying the product of the outer most pair with two plus the square of the middle number, Duplex of abc is $2*a*c+b^2$

Example (Binary):
X=101101, $Y=X^2=101101^2=1111101001$

No	Duplex
1	1*1 = 1
10	(10)*1*0= 00
101	(10)*1*1+0*0=10
1011	(10)*1*1+(10)*1*0= 010
10110	(10)*1*0 + (10)*0*1 + 1*1 = 001
101101	(10)*1*1+(10)*0*0+(10)*1*1=100
01101	(10)*0*1 + (10)*1*0 + 1*1 = 001
1101	(10)*1*1 + (10)*1*0 = 010
101	(10)*1*1 + 0*0 = 10
01	(10)*0*1=00
1	1*1=1

1/00/10/010/001/100/001/010/10/00/1 can be written in the form shown below and finally their sum

```
1 0 0 0 1 0 1 0 0 0 1
0 1 1 0 0 0 1 1 0
  0 0 1 0 0
-----------------------
1 1 1 1 1 1 0 1 0 0 1
```

B. Multiplication using Urdhva Tiryakbhyam

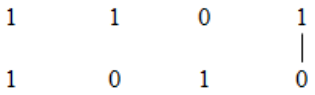
The multiplier is based on an algorithm Urdhva Tiryakbhyam (Vertical & Crosswise) of ancient Indian Vedic Mathematics. Urdhva Tiryakbhyam Sutra is a general multiplication formula applicable to all cases of multiplication. It literally means "Vertically and crosswise". It is based on a novel concept through which the generation of all partial products can be done and then, concurrent addition of these partial products can be done. Thus parallelism in generation of partial products and their summation is obtained using Urdhava Tiryakbhyam as shown in steps below.

Example (Binary):P=X*Y
X=1101, Y=1010
The equations of vedic multiplier are:
X= a3 a2 a1 a0
Y=b3 b2 b1 b0

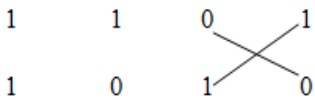
1) P0= a0.b0 =1*0= 0
2) P1=a1.b0+a0.b1= 0*0 +1*1=01
3) P2=a2.b0+a1.b1+a0.b2+P1[1]=1*0+0*1+1*0+0=000
4) P3 = a3.b0 + a2.b1 + a1.b2 + a0.b3 + P2[2 to 1]=1*0+1*1+1*1+0*0+00=010
5) P4= a3.b1 + a2.b2 + a1.b3 +P3[2 to 1]=1*1+1*0+0*1+01=010
6) P5=a3.b2 + a2.b3+ P4[2 to 1]=1*0+1*1+01=010
7) P6=a3.b3 + P5[2 to1]=1*1+01=10
8) Product p ={P6, P5[0], P4[0], P3[0], P2[0], P1[0], P0[0]} (concatenation)=10000010

Various steps are shown in fig. below

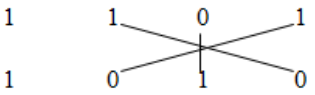
Step 1:



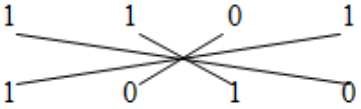
Step 2:



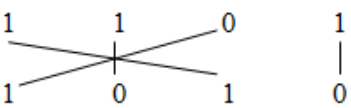
Step 3:



Step 4:

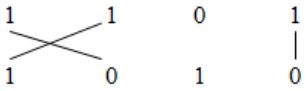


Step 5:

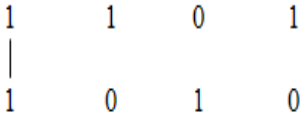


ISSN (Online) 2321-2004
ISSN (Print) 2321-5526
INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 3, Issue 5, May 2015

Step 6:



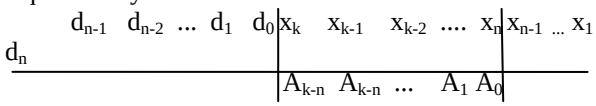
Step 7:



C. Division using Dhwajanka Sutra

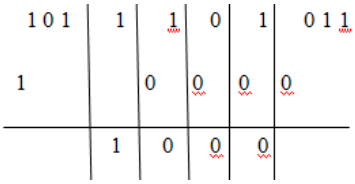
For divison , Dhwajanka sutra is implemented. Dhwajanka – On the top of the flag, is a generalized formula for division. It is based on the formula Urdhva-tiryagbhyam. The actual process of division is performed as follows

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.



2) Only first digit of dividend is divided by the left out digit, quotient and remainder of this division are noted.
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.
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.
5) This process is continued till same number of quotient digits equal to digits in left part of dividend is obtained.
6) Remainder is obtained by subtraction of right part of dividend prefixed by last remainder and cross multiplication of quotient and divisor.

Example (Binary):
1 1 0 1 0 1 1 / 1 1 0 1



Quotient= 1 0 0 0
Remainder=0 0 1 1-0*1-0*0-0*1=0011

IV. RESULT ANALYSIS

Proposed vedic sutras have been simulated and synthesized in Xilinx 13.1 package with Spartan 3 family and XC3S400 device. The simulation results for square of 8-bit binary numbers are shown below:

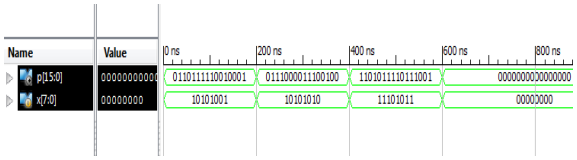


Fig. 1 Simulation result for square of 8-bit binary numbers using Vedic mathematics sutras

Various test cases have been verified for square of a number. Here, x is input signal and p is output signal($p=x^2$)

Case 1: $x=10101001(169_{10})$
$p=0110111110010001(28561_{10})$
Case 2: $x=10101010(166_{10})$
$p=0111000011100100(27556_{10})$
Case 3: $x=11101011(235_{10})$
$p=1101011110111001(55225_{10})$

The simulation results for multiplication of two 8-bit binary numbers are shown below:

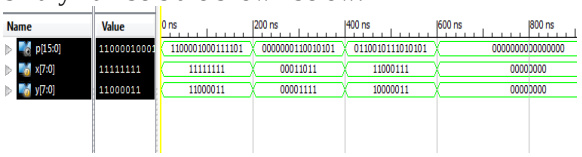


Fig. 2 Simulation result for multiplication of binary numbers using Vedic mathematics sutras

Various test cases with different values of x and y have been tested. Here, x and y are input signals, p is output signal (p=x*y).

Case 1: $x=11111111(255_{10})$, $y=11000011(195_{10})$, $p=1100001000111101(49725_{10})$
Case 2: $x=00011011(27_{10})$, $y=00001111(15_{10})$, $p=0000000110010101(405_{10})$
Case 3: $x=11000111(199_{10})$, $y=10000011(131_{10})$, $p=0110010111010101(26069_{10})$

The simulation results for division of upto 9-bit binary number by divisor of upto 5-bit binary numbers are shown below:

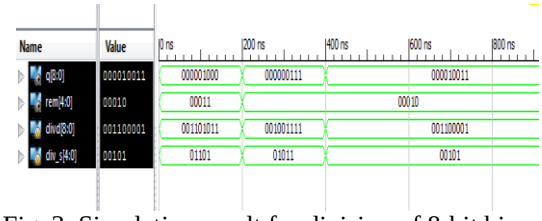


Fig. 3 Simulation result for division of 8-bit binary numbers using Vedic mathematics sutras

Here, divd and div_s are input signals, divd=Dividend and div_s =Divisor
q and rem are output signals, q = Quotient and rem=Remainder

Case 1: divd=001101011, div_s=01101
Quotient=1000, Remainder= 0011
Case 2: divd=001001111, div_s=01011
Quotient=000000111, Remainder=00010
Case 3: divd=001100001, div_s=00101
Quotient=000010011, Remainder=00010

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 3, Issue 5, May 2015

V. CONCLUSION

Various Vedic Mathematics sutras discussed above have been implemented in Verilog HDL and are synthesized and simulated using Xilinx ISE using FPGA family as Spartan 3. The HDL code is written for square of 8 bit binary number, multiplication of two 8-bit binary numbers and division of 9-bit dividend by 5 –bit divisor.

For square of a number, total delay has been reduced from 25.380ns (as in normal multiplication) to 15.859ns in case of using Vedic mathematics sutras.

Number of slices has also been reduced from 72 to 36 out of 4656. or multiplication, total delay has been reduced from 25.380ns to 19.868ns with almost same number of slices.

For division, total delay has been found as 101.503 ns. Number of 8-bit and 16-bit adders/subtractors have also been reduced when design in implemented using Vedic Mathematics Sutras. Future Work: It can be concluded that if these Vedic Mathematics sutras are used for implementation of ECC and RSA algorithms of Cryptography, their performance can be highly improved.

Also, ECC which provide same security level as RSA with smaller key size can be implemented in Xilinx platform using Vedic sutras for square, division, modulus and multiplication.

ACKNOWLEDGMENT

I would like to thank my project guide, **Chiranjeevi G.N**, for giving me permission to submit paper for my work carried out in PESIT, South Campus. I would also like to thank **Dr. Subhash Kulkarni** for introducing me to the field of Vedic Mathematics and FPGA design. I also wish to acknowledge my sincere gratitude to the entire PESIT ECE department faculty for their cooperation in completing the paper.

REFERENCES

[1]. R. Thamil Chelvan and S.Roobini Priya, "Implementation of fixed and floating point division Using Dhvajanka Sutra", International Journal of VLSI and Embedded Systems-IJVES, Vol 04, Issue 02; March - April 2013 ,pp 234-237, ISSN: 2249 – 6556

[2]. Mr. R.G.Kaduskar, 'A new architecture for RSA Algorithm using Vedic Mathematics', 2011 Fourth International Conference on Emerging Trends in Engineering & Technology

[3]. Kuldeep Bhardwaj and Sanjay Chaudhary, 'Implementation of Elliptic Curve Cryptography in 'C'', International Journal on Emerging Technologies 3(2): 38-51 (2012)

[4]. Ankita Soni and Nisheeth Saxena, 'Elliptic Curve Cryptography: An Efficient Approach for Encryption and Decryption of a Data Sequence', International Journal of Science and Research(IJSR),India Online ISSN: 2319-7064

[5]. Greeshma Liz Jose and Sani John , 'VLSI Implementation Of Vedic Mathematics And Its Application In RSA Cryptosystem', International Journal of Innovative Research & Development, Vol 2 Issue 10, October 2013, ISSN: 2278 – 0211

[6]. Ratiranjan Senapati, Bandan Kumar Bhoi and Manoranjan Pradhan, 'Novel Binary divider architecture for high speed VLSI applications', Proceedings of 2013 IEEE Conference on Information and Communication Technologies (ICT 2013).

[7]. Anoop MS 'Elliptic Curve Cryptography - An Implementation Tutorial'.

[8]. Jagadguru Swami Sri Bharati Krishna Tirthji Maharaja, 'Vedic Mathematics', Motilal Banarsidas, Varanasi, India, 1986.

BIOGRAPHIES

Ruchi Anchaliya is an M.Tech student at PESIT South Campus, Bangalore and she is having 4 years industry experience in the field of networking and mobility. Areas of interest are low power VLSI, Optical Networks and Network Security.

Chiranjeevi G.N. is an Assistant Professor at Department of ECE at PESIT South Campus Bangalore. Areas of interest are VLSI, FPGA and Image Processing

Dr. Subhash Kulkarni is a Professor and HOD, of ECE Department at PESIT South Campus, Bangalore and he is having more than 25 years of Academic Teaching Experience. Areas of interest are Math Models in Signal Processing, Image Processing, Control Systems, and Vedic Sutras for fast processor architectures.