An Efficient RSA Algorithm using Pipelined Vedic Multiplier

Parvathy R
PG Student
Department of Electronics & Communication Engineering
Toc H Institute of Science & Technology,
Arakkunnam, Kochi

Prof. G. K. Sadanandan
Associate Professor
Department of Electronics & Communication Engineering
Toc H Institute of Science & Technology,
Arakkunnam, Kochi

Abstract

Multipliers are the essential and abundant part of DSP applications. There are different types of multipliers are used to perform various applications. Array multipliers, Vedic multipliers are two different types of multipliers. Based on the comparative study, it is proved that Vedic multipliers are much faster than array multipliers. The speed of operation is further improved by introducing a pipelined architecture to the conventional Vedic multipliers so that it can be used in very complex multiplication based systems. RSA algorithm is one such popular algorithm which is used for security of networks. It includes several time consuming exponentiation operations based on multiplications. Therefore the proposed pipelined Vedic multiplier based on Urdhva Tiryagbhyam Sutra is applied to RSA to enhance the speed of operation. The design is done using ModelSim and implemented using Xilinx.

Keywords: Cipher text, Modular exponentiation, RSA algorithm, Urdhva tiryagbhyam sutra, Vedic multiplier

I. INTRODUCTION

Multipliers play an important role in today's digital signal processing and various other applications. The implementation efficiency and performance of systems are dependent on the efficiency of the multipliers. Array multiplier, Vedic multiplier and pipelined Vedic multiplier are the different types of multipliers. The array multiplier is a normal multiplier which is based on the shifting and adding operations while Vedic multiplier is based on the natural principles on which human mind works.

Vedic multiplier is based on Indian Vedic Mathematics. The Sanskrit word "Veda" means "Knowledge" and it consists of large number of documents. Vedic Mathematics is the name given by Sri Bharati Krishna Tirtha Maharaj. He explained about 16 Sutras in Vedic Mathematics. The proposed multiplier uses Urdhva tiryagbhyam Sutra, which is a simple multiplication formula which literally means "Vertical and Crosswise". The advantage of using Vedic multiplier is that the partial products are calculated in a single step and there are no time consuming shifting and adding operations. Introduction of delay stages in the normal Vedic multiplier allows the pipelining of operation and thus further decreases the delay associated with the multiplier. Therefore such a pipelined Vedic multiplier can used in systems which require complex multiplication operations.

The application of the high speed multiplier mainly includes the cryptographic systems. Cryptography is the science of using mathematical equations for encryption and decryption of data. By using this technique, the information cannot be read by unintended recipients. Public key cryptography and private key cryptography are the two kinds of cryptographic techniques. Public key cryptography system is a well-known method which is used in many applications such as smart cards, digital certificates etc. RSA (Rivest Shamir Adleman algorithm) is one of the widely used public key algorithms developed in 1977 by Ron Rivest, Adi Shamir and Len Adleman. It is one of the simplest and safest algorithms that use different keys for encryption and decryption. The most time consuming operation in RSA algorithm is modular exponentiation operations that include several modular multiplication operations. The pipelined Vedic multiplier is used here to speed up the operation thus the overall system provides an efficient technique for enhancing security in networks.

II. ARRAY MULTIPLIER AND VEDIC MULTIPLIER

Array multiplication and Vedic multiplication are two important types of multiplication techniques. A 4x4 multiplier and 8x8 multiplier based on both these techniques are designed to compare the results. Both the designs are simple however their delays are different.

A. Array Multiplier:

Array multiplier is well known due to its regular structure. Multiplier circuit is based on add and shift algorithm. Each partial product is generated by the multiplication of multiplicand with one multiplier bit. The partial product are shifted according to

their bit orders and then added. The addition can be performed with normal carry propagate adder. N-1 adders required N is the multiplier length.

A 4 bit array multiplier is shown in Fig. 1. This consists of large number of AND array to obtain the partial products and 4 half adders and 6 full adders are used to added up these partial products to obtain the final product bits. Each stage involves the transfer of carry from one adder to the next.

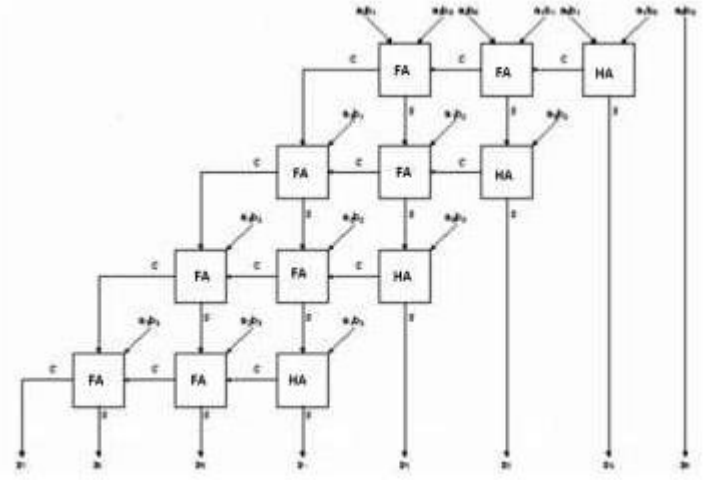

Fig. 1: A 4x4 array multiplier

B. Vedic Multiplication Technique:

The Vedic mathematics is based on the natural principles on which human mind works. The importance of these Vedic formulae lies in the basic fact that it reduces the typical calculations in the conventional mathematics to very simple ones. The proposed multiplier is based on Urdhva Tiryagbhyam Sutra which is literally means "vertical and crosswise". The concept of this method is that the product bits can be obtained by concurrent addition of partial products. Fig. 2 shows the 4x4 Vedic multiplication techniques.

1) 4x4 Vedic Multiplier:

Consider the multiplication of two numbers a3a2a1a0 and b3b2b1b0. Vertical and crosswise multiplication is take place to obtain the final result. In every step, LSB bit of sum is stored in product and higher order bits considered to be carry bits for next stage operation and final result will be obtained as p7p6…p0. All the partial products are obtained parallel and shifting of partial products is eliminated in case of Urdhva Tiryagbhyam Sutra, hence it is more efficient.

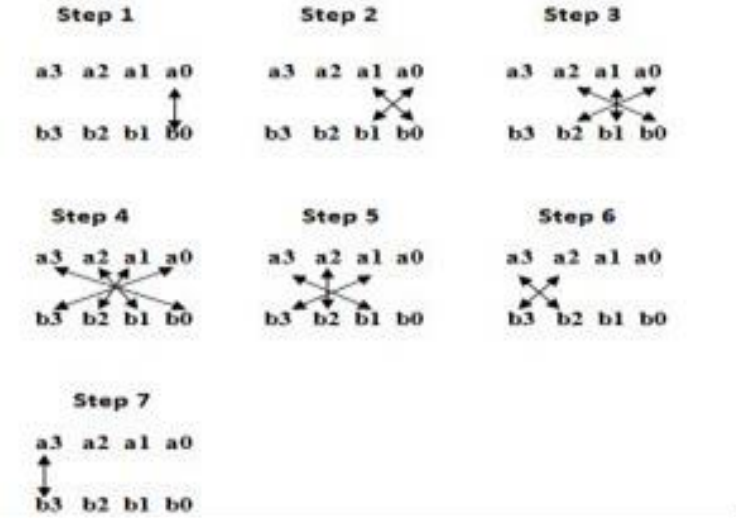

Fig. 2: 4x4 Vedic Multiplication techniques

The equations of 4x4 Vedic multiplier are given:

1) P0=a0b0
2) P1=a1b0+ a0b1
3) P2=a2b0+a1b1 +a0b2+a0a1b0b1
4) P3=a3b0+ a2b1+ a1b2+ a0b3+ carry from P2
5) P4=a3b1+ a2b2+ a1b3+ carry from P2+carry from P3

6) P5=a3b2+ a2b3+ carry from P4+carry from P3
7) P6=a3b3+ a1a2b1b2+ carry from P4
8) P7=carry from P6

Then the multiplier output will be in the form given below.

P=P[0] & P[1] & P[2] & P[3] & P[4] & P[5] & P[6] & P[7].

The architecture in Fig. 3. is used for generating the outputs of 4x4 multiplier. Here 6 adders are used to add up the partial product terms generated. It is a time consuming structure since the carry propagates through all the stages.

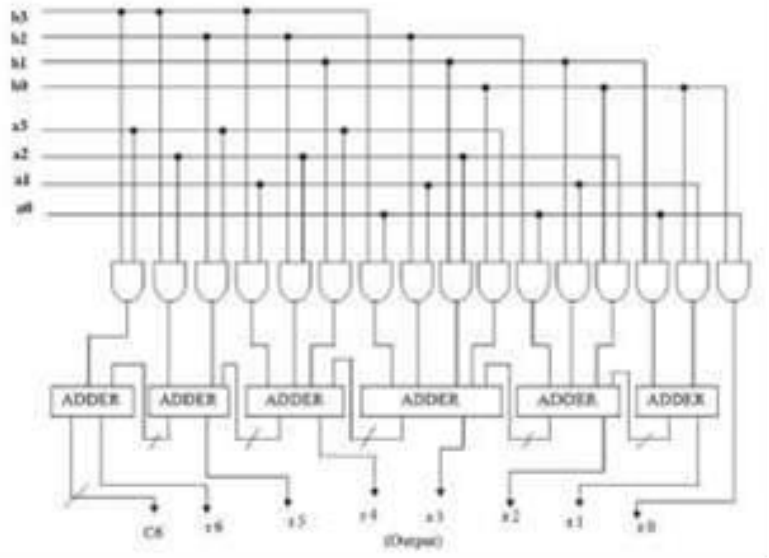

Fig. 3: 4x4 Vedic multiplier structure

2) 8x8 Vedic multiplier:

Similar to 4x4 Vedic multiplier, 8x8 multiplier is also designed using a set of adders to obtain the products parallel. But in each adder, higher order bits of the results are taken to the adjacent adders to obtain the final result. This causes 14 cycles of delay since the critical path involves all the adders.

III. PIPELINED VEDIC MULTIPLIER

4x4 pipelined Vedic Multiplier: From the equations of a 4x4 Vedic multiplier, it is understood that the carry propagated to next adders in some cases. According to this, it can be divided into various stages of pipeline and 4 stages of pipeline operation are done here to reduce the critical path delay. As the number of stages increases speed increases but it leads to area overhead, hence minimum number of registers is preferred.

The use of registers is shown in Fig. 4. In this proposed model, input of the first stage are processed and result is kept in 1st level register, simultaneously other stage inputs are fed to first level registers. At the second cycle of clock, 2nd stage inputs are processed, and the obtained results are placed in 2nd level registers and simultaneously next stage inputs are fed to 2nd level registers. Finally, the output results are obtained after 4th clock cycle. In the same way 2nd data operand are processed with one stage lagging and hence after 5th clock cycle, output of 2nd data operand are obtained.

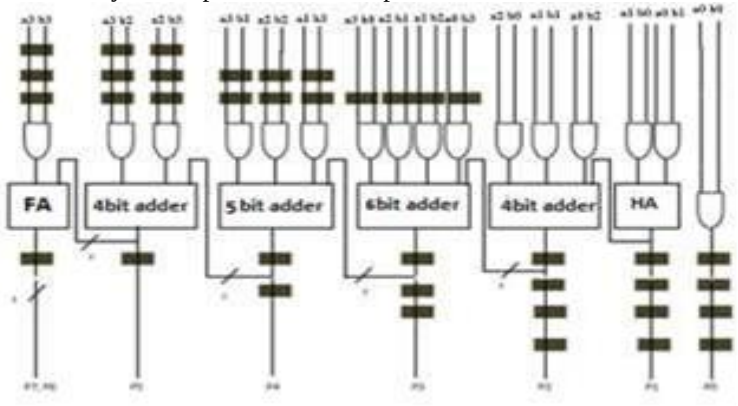

Fig. 4: 4x4 Pipelined Vedic multiplier structure

1) 8x8 pipelined Veic Multiplier:

The 8x8 Vedic multiplier involves a large critical path delay. In order to reduce this delay, pipelining can be used. According to the carry propagation, 12 stage pipelining is introduced in the 8 bit Vedic multiplier as shown in Fig. 5.

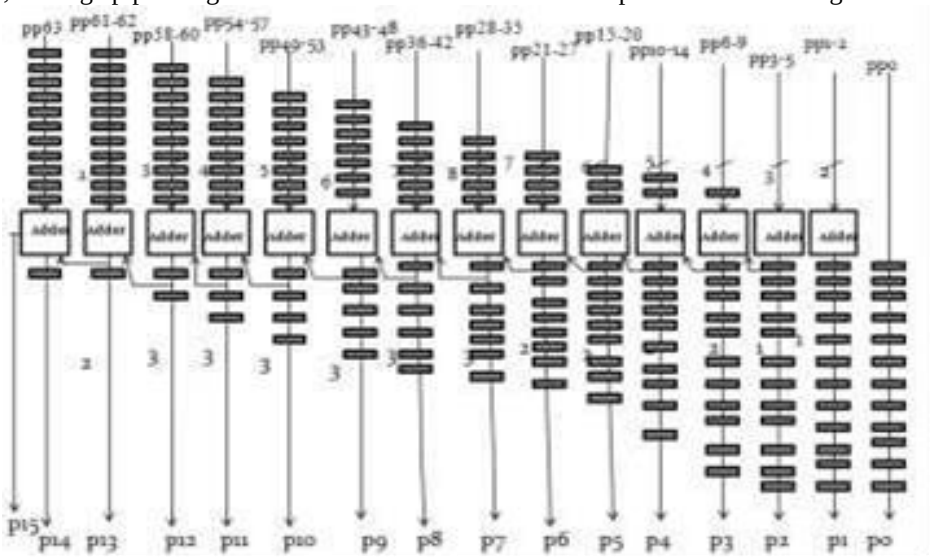

Fig. 5: 8x8 Pipelined Vedic multiplier structure

IV. RSA ALGORITHM

RSA is a very simple algorithm for efficient transmission of data through networks. The encryption and decryption are based on two mathematically related keys and it is difficult to decrypt by unknown parties. The main RSA encryption and decryption algorithm are given.

A. Encryption and Decryption:

Encryption is the process of converting a text to a format which is not directly readable. This conversion involves some mathematical operations and it is based on two keys. After the key generation step, the encryption and decryption are done using modular exponentiation operation.

Plain text M is encrypted to cipher text C by the equation:

$C = M^e \bmod n$ (1)

The plain text M is recovered from the cipher text C by the equation:

$M = C^d \bmod n$ (2)

Here n,e and d are the values obtained through key generation process.

B. RSA Key Generation Algorithm:

The RSA key generation algorithm is based on two large numbers. The algorithm is as follows.

- Choose two large prime numbers p and q.
- Compute n=pq.
- Calculate $\phi(n) = (p-1)(q-1)$
- Select the public exponent e€ {1, 2. . . (n)−1} Such that GCD (e, $\phi(n)$) = 1.
- Compute the private key d such that dxe ≡ mod ϕ (n)

Output: Public Key: $K_{pub} = (n, e)$

Private Key: $K_{pr} = (d)$

C. Modular Exponentiation Operation:

Modular exponentiation operation in RSA involves series of modular multiplication and squaring operations. In this algorithm, the exponents are scanned from most significant bit to least significant bit. This algorithm can be explained as follows.

Square and Multiply Algorithm: Input: M, e, n

Output: $C=M^e \bmod n$

If $e_{k-1}=1$ then C=M else C=1 for i= k-2 down to 0

C=C X C

If $e_i=1$ then C= CX M

V. RESULTS AND CONCLUSION

The multiplication in RSA algorithm is very critical operation. This calls for the need for a fast multiplier. The array multiplier, Vedic multiplier and Pipelined Vedic multiplier are implemented, the delays were analyzed and it is found that Pipelined Vedic multiplier performs faster than others. The delay analysis is shown in tables 1 and 2.

Table - 1
Delay Analysis of 4x4 Multipliers

Type of Multiplier	*Delay*
4 bit array	*22.175ns*
4 bit Vedic	*4.37ns*
4bit pipelined	*1.452ns*

Table - 2
Delay Analysis of 8x8 Multipliers

Type of Multiplier	*Delay*
8 bit array	*32.138ns*
8 bit Vedic	*19.642ns*
8 bit Vedic pipelined	*1.181ns*

In case of 4 bit multiplier, the pipelined structure is about 15 times faster than normal array multiplier. In case of 8 bit multipliers, pipelined structure improves the speed about 25 times of array multiplier. Therefore, the RSA algorithm can be made faster by applying this pipelined architecture into this. The simulation result is shown in Fig. 8.

REFERENCES

[1] G.Ganesh Kumar, V.Charishma, "Design of High Speed Vedic Multiplier using Vedic Mathematics Techniques",International journal of Scientific and Research Publications, Volume 2,Issue 3, March 2012.
[2] Poornima M, Shivaraj Kumar Patil, Shivukumar , Shridhar K P , Sanjay H, " Implementation of Multiplier using Vedic Algorithm", International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 5, May – 2013.
[3] Prakash Pawar, Varun. R, Suma M. S, "Implementation Of High Speed Pipelined Vedic Multiplier", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-2, Issue-6, May 2013.
[4] Sushanta Kumar Sahu , Manoranjan Pradhan, "FPGA Implementation of RSA Encryption System", International Journal of Computer Applications (0975 – 8887)Volume 19– No.9, April 2011.
[5] Chiranth E, Chakravarthy H.V.A, Nagamohanareddy P, Umesh T.H, Chethan Kumar M, "Implementation of RSA
[6] Cryptosystem Using Verilog", International Journal of Scientific & Engineering Research, Volume 2, Issue 5, May-2011 1 ISSN 2229-551
[7] Shahina M. Salim1, Sonal A. Lakhotiya, "Implementation of RSA Cryptosystem Using Ancient Indian Vedic mathematics", International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438
[8] G.Suman , P.Anuradha, "RSA Algorithm and LSB Steganography", International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 10, October – 2013 ISSN: 2278-0181.