IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013
ISSN: 2320 – 8791
www.ijreat.org

Analyzing the performance of RC6 using Complex Vedic Multiplier

[1]Thenmozhi.C & [2]Kishore Sonti
[1,2] Department of Electronics and Communication Engineering, Sathyabama University, Chennai, Tamil Nadu, India.

Abstract

In this thesis we proposed the performances of RC6 Algorithm using Complex Vedic Multiplier. RC6 are widely used cryptographic algorithm for data security. Cryptography is the art of converting normal text to cipher text in order to protect the data. A system which consists of Encryption and Decryption is known as Cryptosystem. Encryption does not hide datas, it just make the contents unreadable by the casual readers. Decryption process are helpful to convert unreadable content into original text by the help of keys. Keys play a vital role in Cryptographic Algorithms. Size of the key varies depend on the features of Algorithm. Security of the Cryptography depends on the key which is used in both encryption and decryption. The performance of RC6 Algorithm improved using Vedic Sutras in Multipliers. Generally Vedic Mathematics reduce the partial products of most multipliers for better performance. Sutras such as "Urdhvat-tiryakbyham" and "Nikhilam Navatascaramam Dasatah" are well known sutras for multiplication, which are used to increase the efficiency of RC6.

*Keywords: RC6 Algorithm, Vedic Multiplier, Cryptography***.**

I.INTRODUCTION

RC6 is one of the best AES algorithm and simple cipher used for data security. It involves numerous evaluation and adequate security. The improved efficiency and security is obtained using Vedic Sutras. The Sutras of Vedic Mathematics are implemented in multipliers. The Encryption and Decryption of RC6 are best evaluated using Vedic Mathematics.

In today mechanism, RC6 Algorithm is known to be the one important and best algorithm for data security. Many works are developed for data security in internet applications and other applications. For improved speed and best evaluation, Vedic Mathematics are involved in these kind of algorithms. Out of 16 sutras, two best are selected and involved in project

II CRYTOGRAPHY

In Cryptography RC6 is a symmetric key block cipher derived from RC5. Cryptography means "Secret Writing" which provide security for any information or datas. It is the method of converting the given data into other form which cannot be recognize by third party. Encryption and Decryption are involved in Cryptography. Encryption is the process of converting Plain text into Cipher text. Decryption is the process of converting Cipher text back to Plain text. For Information security systems in internet and network applications, Encryption algorithms are necessary. Meanwhile these algorithms consume time power and memory. Plain text, Key and Cipher text are the common terms of Cryptography. Plain text is the text by sender. Cipher text is the text given to receiver. Key plays an important role in encryption algorithms. If length of the key is small then it is easy to break. Longer key are difficult to break.

Cryptography helps to rend the messages from attackers by various transformations such as Substitution and Transposition. Substitution means data in the plain text is converted into cipher text by the process of substitution. Transposition means data in the plain text is converted into cipher text by the process of reposition. These processes are helpful by the user to increase the security. Also these processes involved in both encryption and decryption.

Cryptography is classified into Symmetric and Asymmetric. Symmetric Cryptography uses common key (known as private key) for both encryption and decryption. Here Decryption is the inverse of Encryption.

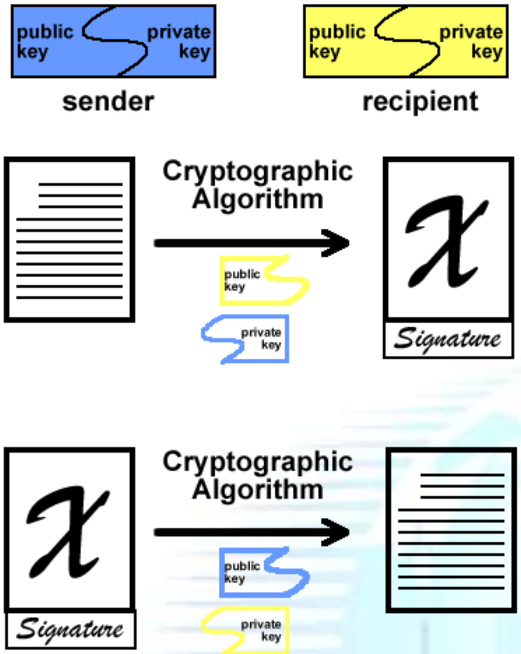
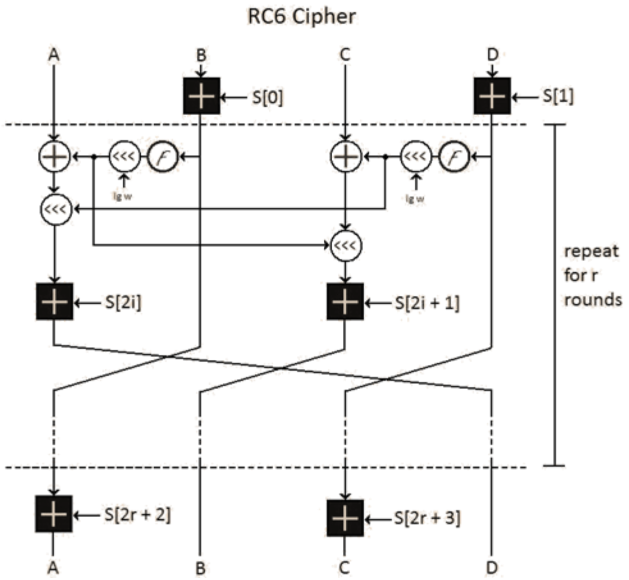


Figure:cryptography

Many Algorithms are developed based on Symmetric Cryptography. Such as RC6, DES, 3DES, RC6, Blowfish and AES. Asymmetric Cryptography has two keys private key and public key. Public Key is used for encryption and private key is use for decryption. Public key encryption is based on mathematical functions. Such as RSA and Digital Signatures. Asymmetric encryption techniques are almost 1000 times slower than symmetric techniques because they require more computational processing power. Asymmetric key encryption is used to solve the problem of key distribution.

III RC6

RC6 is a very simple cipher with excellent security credentials. In many situations and environments its performance is at least equal to, and in several places better than, the other AES finalists. RC6 has a block size of 128 bits and supports key sizes of 128, 192 and 256 bits, and 20 rounds but, like RC5, it can be parameterised to support a wide variety of word-lengths, key sizes and number of rounds. RC6 is very similar to RC5 in structure, using data-dependent rotations, modular addition and XOR operations; in fact, RC6 could be viewed as interweaving two parallel RC5 encryption processes. However, RC6 does use an extra multiplication operation not present in RC5 in order to make the rotation dependent on every bit in a word, and not just the least significant few bits. RC6 has not been selected for the AES, it is not guaranteed that RC6 is royalty-free.



Encryption/Decryption

```
// Encryption/Decryption with RC6-w/r/b
//
// Input:Plaintext stored in four w-bit input registers A, B, C & D
//     r is the number of rounds
//     w-bit round keys S[0, ... , 2r + 3]
//
// Output: Ciphertext stored in A, B, C, D
//
// '''Encryption Procedure:'''

    $B = B + S[0]$
    $D = D + S[1]$
    for i = 1 to r do
    {
        $t = (B*(2B + 1)) <<< \lg w$
        $u = (D*(2D + 1)) <<< \lg w$
        $A = ((A \oplus t) <<< u) + S[2i]$
        $C = ((C \oplus u) <<< t) + S[2i + 1]$
   $(A, B, C, D) = (B, C, D, A)$

    }
```

```
        $A = A + S[2r + 2]$
        $C = C + S[2r + 3]$

// '''Decryption Procedure:'''

        $C = C - S[2r + 3]$
        $A = A - S[2r + 2]$

        for $i = r$ downto 1 do
        {
           $(A, B, C, D) = (D, A, B, C)$
            $u = (D*(2D + 1)) \lll \lg w$
            $t = (B*(2B + 1)) \lll \lg w$
            $C = ((C - S[2i + 1]) \ggg t) \oplus u$
            $A = ((A - S[2i]) \ggg u) \oplus t$
        }
        $D = D - S[1]$
        $B = B - S[0]$
```

The above calculations are very important for RC6 Algorithm. It tells about the mechanism of RC6 Algorithm.

Diffusion means that any change of bits in a plain text to enhance complexity between the plain text and the cipher text. In a block encryption/decryption system diffusion can be achieved by repeatedly implementing a specific permutation and then execute a functional operation. Confusion can be achieved by manipulating the relations between cipher text and sub key to be more complicated, leaving no chance of existence of direct linear relationship.

Whitening technique of XORing key material before the first round and after the last round, it was shown that whitening substantially increases the difficulty of key search attacks against the remainder of the cipher. There are three round stages available. They are Pre Whitening, R- rounds and Post Whitening. Pre-Whitening helps to remove the inferences of part of the input to the first round of encryption. R-rounds use integer multiplication, quadratic equation and fixed for bit shifting. Integer Multiplication ensures that the bits used for rotation amounts depend on the bits of x, which is a word or register. Quadratic Equation increases the avalanche of changes per round. The bit shift complicates more advanced cryptanalysis attacks. Post Whitening helps to remove the inferences of part of the input to the last round of encryption.

IV VEDIC MATHEMATICS

Vedic mathematics is the name given to the ancient system of mathematics, or, to be precise, a unique technique of calculations based on simple rules and principles with which any mathematical problem can be solved – be it arithmetic, algebra, geometry or trigonometry. The system is based on 16 Vedic sutras or aphorisms, which are actually word formulae describing natural ways of solving a whole range of mathematical problems.

Vedic mathematics was again rediscovered from the ancient Indian scriptures between 1911 and 1918 by Sri Bharati Krishna Tirthaji (1884-1960), a scholar of Sanskrit, mathematics, history and philosophy. He studied these ancient texts for years and, after careful investigation, was able to reconstruct a series of mathematical formulae called sutras. Bharati Krishna Tirthaji, who was also the former Shankaracharya (major religious leader) of Puri, India, delved into the ancient Vedic texts and established the techniques of this system in his pioneering work, Vedic Mathematics (1965), which is considered the starting point for all work on Vedic mathematics.

According to Mahesh Yogi, The sutras of Vedic Mathematics are the software for the cosmic computer that runs this universe. A great deal of research is also being carried out on how to develop more powerful and easy applications of the Vedic sutras in geometry, calculus and computing. Conventional mathematics is an integral part of engineering education since most engineering system designs are based on various mathematical approaches. The need for faster processing speed is continuously driving major improvements in processor technologies, as well as the search for new algorithms.

III.EXISTING SYSTEM:

In the existing system RC6 Algorithm is implemented for many security and internet application. As mentioned previously RC6 Algorithm termed as one of the most secured symmetric key algorithm. Several works have already implemented using RC6 algorithms. The performance of RC6 Algorithm is greatly improved in each and every work. The improvement in performance is measured by means of security. The security level for these kind of Algorithms is measured by decryption process.

Meanwhile several works regarding Vedic Mathematics are also developed. Vedic Mathematics mostly applied in electronic systems or devices where multipliers are available.

In Multipliers delays are greatly prohibited by using Vedic Mathematics. Totally 16 sutras are available in Vedic Mathematics. Out of 16 sutras, two well known sutras are available for multipliers alone. The main advantage of using Vedic sutras in multipliers is to reduce partial products. Reduction of partial products helps to improve the performance and efficiency.

IV. PROPOSED SYSTEM:

In this paper we proposed RC6 Algorithm using Vedic Sutras such as **"Urdhvat-tiryakbyham" and "Nikhilam Navatascaramam Dasatah".** The security level of RC6 Algorithm is greatly improved using these sutras. The multipliers in RC6 Algorithm are replaced by Vedic Sutras. These Vedic Sutras helps to reduce the partial products. Thus the efficiency of RC6 Structure is greatly improved. The performance of RC6 Algorithm is compared with two sutras separately. Finally best one is studied and analyzed using Xilinx tool and ActiveHDL.

VI. RESULTS AND CONCLUSIONS:

Thus the performance of RC6 algorithm with Vedic Mathematics is analyzed and compared two different sutras. Vedic Sutras are implemented to reduce the partial products of multipliers in RC6 structure. By reducing these partial products help to improve the performance and efficiency of RC6 structure. The performance of RC6 structure is measured by means of security provided.

VII. REFERENCE:

[1] Moses, S.L.G-VLSI Design, Thilagar, M. in: Electronics Computer Technology (ICECT), 2011 3rd International Conference.

[2] Gil-Ho Kim-Dept of Comput. Eng., Pu Kyong Nat. Univ., Pu Kyong, Jong-Nam Kim ;Gyeong-Yeon Cho Advanced Communication Technology, 2009. ICACT 2009. 11th International Conference

3] Erica Mang et al (1997), the National Institute of Standards and Technology (NIST).

[4] Improved Analysis of Some Simplified Variants of RC6 (1999) by Scott Contini , Ronald L. Rivest , M. J. B. Robshaw , Yiqun Lisa Yin.

[5] Sriraman, L. Dept. of ECE, Oxford Eng. Coll., Trichy, India Prabakar, T.N. Recent Advances in Information Technology (RAIT), 2012 1st International Conference

[6] **):** El-Fishawy, N.A. Menofia University El-Danaf, T.E. ;Abou Zaid, O.M. Electrical, Electronic and Computer Engineering, 2004. ICEEC '04. 2004