Executive summary of Minor Research Project

Name of the Principal Investigator: Sreeja K
Title of the Project: Applications of Vedic Mathematics in Cryptography
UGC Ref. No.: F. 2369-MRP/15-16/KLMG002/UGC-SWRO

Introduction

Vedic Mathematics is India's Gift to World. Vedic mathematics provides an innovative, simple and flexible technique of computation of almost all mathematical operations. In this era of digitalization, increasing speed of arithmetic operations results in increasing the efficiency of a digital design. Vedic mathematics reduces the steps required in arithmetic computations. This observation has motivated researchers to design various architectures based on Vedic math. Vedic mathematics sutras are proven to improve the conventional architecture in computer applications with respect to computational speed and utilization of power.

A literature survey was performed on application of Vedic mathematics in the area of computation and cryptography in specific. It is observed that the sutras of Vedic mathematics, especially Urdhva Triyagbhyam, Nikhilam sutra, Dwandwayoga Sutra, Dhwajanka Sutra are widely used to simplify and fasten the computation. In literature, techniques are shown to be useful in high speed processing and low area design. The multipliers designed using Vedic mathematic techniques are twice as fast as the ones using the popular methods of multiplication. Techniques such as Urdhva Triyagbhyam and Nikhilam sutra, which are used for multiplication, were shown to improve upon power consumption.

Design of Crypto systems.

Several cryptographic systems were designed using Vedic mathematical techniques for the implementation in hardware circuitry. RSA (Rivest–Shamir–Adleman), which is one of the popular public-key crypto-systems, shows performance improvement with the use of Vedic mathematic multiplication

techniques. These techniques, when used in RSA encryption and decryption, has shown improvement over the typically used modular multiplication algorithms. Advanced Encryption Standard (AES) is another efficient and popular cryptographic algorithm used in industrial applications. Methods have been proposed for the mix columns and inverse mix columns operation in AES cryptography based on Vedic mathematic techniques. These methods help in providing diffusion of data in an efficient way. Vedic mathematic techniques are successfully used in securing on-line payment systems. The use of Steganography techniques in fund transfer systems helps in shielding the customer data and preventing identity theft.

In several recent literature, it was shown that the use of Vedic mathematic techniques brings improvement to cryptographic systems and enable us to have high speed systems. It was shown that the use of Urdhva Triyagbhyam helps in a parallel generation of intermediate products. It gives a regular and parallel structure to hardware implementations and is realized easily on silicon. DSP operations take lesser time with Vedic techniques compared to that of inbuilt Matlab functions and give better results. These techniques help in calculating deconvolution with lower time-delays and lower complexity compared to popular techniques. Vedic division algorithms give appreciably constant computation time irrespective of the dividend size.

The challenge of computing with encrypted messages is quite fascinating and has captivated the attention of majority of researchers in the domain. In the past few decades, theoretical and practical advances in this field have been impressive. The usage of these techniques in real-world applications intend to build systems with suitable trade-off between security and efficiency.

VLSI in cryptosystems

The long and complex processes required by cryptography often call for custom hardware support. Implementing cryptographic algorithms using VLSI help to increase the Security, Reduce Power Consumption, Reduce area of the Chip. Very Large Scale integration is one important domain where Vedic sutras brought a considerable progress. Vedic sutras can be applied to several different basic units

involved in VLSI systems such as multipliers, floating point units and ALU. The report reflects upon the understanding of the domain obtained through the study performed in this domain.

To facilitate secure network and data storage cryptography algorithms play an important role. These algorithms are of two types namely - asymmetric key cryptography such as RSA (Rivest–Shamir–Adleman) algorithm and symmetric key algorithms such as AES (Advanced Encryption Standard). In case of public key (asymmetric key cryptography) another Elliptic Curve Cryptography is getting much attention in this era. This is due to its ability to offer equal security for a smaller size of the key. This reduces processing overhead considerably, in comparison with other public key cryptography algorithms. Other advantages include high speed, less consumption of power and reduced size of the certificates. These properties make the algorithm useful for wireless networks.

For encryption technique using Advanced Encryption Standard (AES) a important step in computations is the Galois field multiplication during the mix column step. This step is laborious and requires high consumption of power causes the mix column step and inverse of it to be expensive in terms of the processing power. This can considerably be simplified by simplifying the basic operation of matrix multiplication. To achieve such a simplified Galois field multiplication, the Urdhva Tiryakbhyam Sutra of Vedic Mathematics can be incorporated into the architecture. This will make sure that the operations of mix columns and its inverse will require lesser speed and area on the chip. The key to this improvement is the algorithm's ability to generate product of two numbers in a one step. In addition, as the multiplication of two single bits is a single AND operation in implementation, this approach results in a design that is area efficient and speed efficient.

Conclusion

The study showed the potential of Vedic mathematic techniques in cryptography and several signal processing applications. The information and the insights achieved over the study should be helpful in conducting further investigations on benefits of Vedic mathematic algorithms.