International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 5.22 (SJIF-2017),e-ISSN:2455-2585
International Conference on
Recent Explorations in Science, Engineering And Technology (ICRESET'19)
Volume-5, Special Issue-March, 2019.

ANALYSIS OF OPTIMIZATION METHODOLOGY FOR SECURE CRYPTOSYSTEM USING LOW POWER VLSI DESIGN TECHNIQUES

Rithmi Mitter [1], V Rajeswari[2]

Assistant Professors, Department of ECE,
KGiSL Instsitute of Technology, Coimbatore, India.

Abstract— Security in today's environment becomes a drastic issue in communication. For secure transmission of data or image in open network, encryption is very important methodology. Through encryption we can prevent our data or image from unauthorized access during transmission. In recent years many encryption methods have been proposed and used to protect data. Image encryption and decryption using chaotic map and BB equation is one of the best image encryption methods. VLSI architecture for the proposed algorithm is also available and is implemented in FPGA using VHDL language in Xilinx ISE VLSI software. This implementation can be further modified with low power VLSI criterions i.e. how the power consumption can be reduced with less delay and reduced area .To perform the encryption process more secure and fast many ideas has been suggested and implemented. The architecture has been implemented using different adders and it is always found that there exist tradeoffs between delay and area of implementation. In this paper, a comparative study of different architecture used to reduce the power consumption with the help of various adders such as carry look ahead adder, carry bypass adder, carry save adder etc has been carried out and thus have quoted the tradeoffs between delay and area of architectures implemented. Various power reduction techniques in digital VLSI are also discussed and implemented. With this study the best approach suitable for different application can be easily recognized and the same can be implemented to increase the efficiency.

Keywords: BB equation, chaotic map, cryptography, image encryption, image decryption, VLSI.

INTRODUCTION

Recent information and communication technologies require adequate security. Cryptology is the technology that aims to provide information security in the digital world. Information security comprises many aspects, the most important of which are confidentiality and authenticity. Confidentiality means keeping the information secret from all except those who are authorized to learn or know it. Authenticity involves both ensuring that data have not been modified by an unauthorized person (data integrity) and being able to verify who is the author of the data (data origin authentication). Cryptology is divided into two closely related fields as cryptography and cryptanalysis.

Cryptography aims at how to design more secure and fast encryption algorithms, and cryptanalysis tries to find security weaknesses of existing algorithms and studies whether or not they are vulnerable to some attacks. In the current scenario the technologies have been advanced. People prefer using the internet as the primary medium to transfer data from one end to another across the internet. There are many possible ways to transmit data using the internet like: via e-mails, sending text and images, etc. However, one of the main problems with sending data over the Internet is the 'security' and authenticity. Information security basically means protection of data from unauthorized users or attackers. Cryptography is one of the techniques for the information security. Picture encryption is a technique that convert original image to another form that is difficult to understand. Anyone can access the content only by knowing the decryption key. Picture encryption has applications in corporate world, health care, military operations, and multimedia systems. Encryption method is a method of transforming original data, called plaintext or clear text, into a form that appears to be random and unreadable, which is called cipher text. Plaintext will be in a form that can be understood by a person or by a computer. Once it is transformed into cipher text neither human nor machine can properly process it until it is decrypted. Decrypted image is changing it back to its original form. The encryption and decryption process block diagram is as shown in Figure 1.

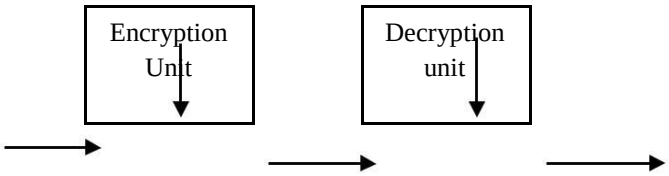

Figure 1. Block diagram of Encryption and Decryption

The original message for encryption is called plaintext, and the encrypted message is called cipher-text, which is denoted here by P and C, respectively [1]. The encryption of a image can be described as C=EK1(P), where K1 is the key used for encryption process and E(.) is the encryption function. Similarly, the decryption procedure is P=DK2 (C), where K2 is the decryption key and D(.) is the decryption function. When K1=K2, the cipher is called a private-key cipher or a symmetric cipher and when K1=!K2, cipher is called a public-key cipher or an asymmetric cipher [2]. In this paper a comparative study of image encryption and decryption based on chaotic map and BB equation using different adder is proposed and a comparative study is done on various approaches to reduce power.

CHAOTIC KEY BASED APPROACH (CKBA)

The commonly used method of protecting digital documents is to scramble the content so that the true message of the documents is unknown. There are different techniques to achieve this for example compression, digital watermarking, steganography and cryptography. One among different methods used for image Encryption is the chaos key based approach. Chaos refers to randomness and it is defined as a study of nonlinear dynamic system. The chaos systems are characterized mainly sensitivities to initial conditions and other system parameters. Due to this sensitiveness, the system acts very randomly. One of the advantages of the chaotic encryption approach include: high flexibility in the encryption system design, availability of huge number of variants of chaotic systems, large, complex and numerous possible encryption keys and simpler design. This ensures to provide strong encryption without compromising the usability system in terms of speed and robustness.

Based on chaotic key based approach gray levels of each pixel is xored or xnored to one of the two keys (key 1 and key 2) [3]. This technique has high hardware utilization efficiency, low hardware cost and high computing speed but has increased bit rate and computation time is more. Chaotic key based cryptography process assume that the system security is derived from the fact that a cryptanalyst does not know the encryption system and hence it is nearly impossible to attack it with knowledge of cipher text alone. Systems that gain their security in this way are not worth very much as sooner or later the system will be known.

The chaotic function that is used is given by

$X(i+1) = \mu x(i)\,(1-x(i))$ (1) Where $\mu = 3.9$

Figure 2 shows the architecture of the chaotic binary sequence generator (CBSG). It is composed of two multiplier, one subtractor, one D flip flop and one multiplexer. The time taken to generate a chaotic bit string value is assumed to be the time for two multiplications and one multiplexing [3].

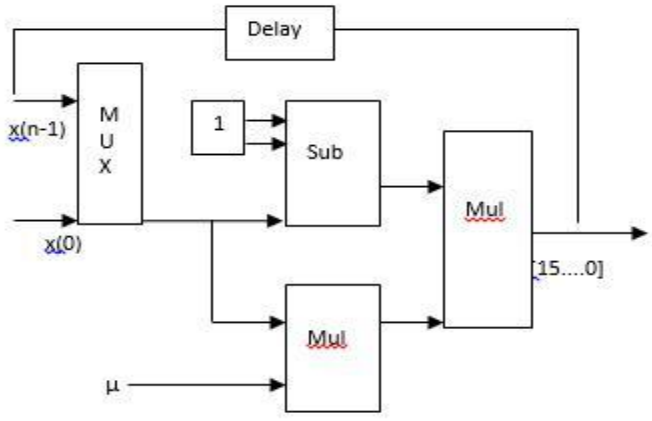

Figure 2. Architecture of CBSG

BB EQUATION

For the introduction of non-linearity in any system we use BB equation. It employs block size that is variable and here fixed key size is not employed and a key of smaller size is employed. The key space is larger. It provides larger key space as the size of key is limited by hardware/software and real time speed considerations. It can significantly employ keys of smaller size as the key is distributed among one primary key p and two secondary keys.

Brahmagupta–Bhãskara (BB) equation is a quadratic Diophantine equation of the form NX2+K=Y2, where K is an integer and N is a positive integer. A similar case of the BB equation with K = 1 is also known as Pell equation in literature [4]. This equation used in the Galois Field GF(p), where p is an odd prime has some practically useful properties.

The BB equation in Galois field GF(p), can be described as:

$$(nx2+1)\ p = (y2)\ p \qquad (2)$$

The subscript p stands for modulo operation by p on the argument values of the expressions.

For obtaining a valid quadratic residues solution of the BB equation in Galois field GF(p), Equation (2) can be described as

$$((nx2)p)p+1 = (y2)\ p$$

This equation can also be written as

$$(nqx+1)p = (qy)p \qquad (3)$$

Where qx and qy are the quadratic residues solution of the BB equation in GF(p).

For solving the BB equation, find a possible pair (x,y) so the equation (1) is satisfied for given n and p.

Once x and y are found, and then qx and qy are computed as

qx=(x2)p, qy=(y2)p

The encryption process using BB equation is as follows:

n corresponds to the plaintext in a block that is being encrypted.

p corresponds to the primary secret key used in the encryption of the plaintext in a block.

The cipher text that corresponds to n is the pair (qx,qy) of the corresponding BB equation.

LOW POWER TECHNIQUES

Power reduction can be implemented at different levels of design levels like system level, architectural level, gate level, circuit level and the technology level. In system level inactive modules may be turned off to save power. At the architectural level methods like parallel hardware may be used to reduce global interconnect and allow a reduction in supply voltage without degrading system throughput. Clock gating is commonly used at the gate level and a variety of design techniques can be used at the circuit level to reduce both dynamic and static power.

SOURCE OF POWER DISSIPATION

The main sources of power consumption in a CMOS chip is classified as static and dynamic power dissipation. Out of which the major source of power consumption in CMOS is dynamic power consumption caused by the actual effort of the circuit to switch. The first order approximation of the dynamic power consumption of CMOS circuitry is given by the formula: P= C*V2*f, Where P is the power, C is the effective switch capacitance, V is the main supply voltage, and f is the frequency at which the system operates. The power dissipation occurs by the charging and discharging of the circuital node capacitances found on the output of every logic gate. Every low to high logic transition in a digital circuit exhibits a change of voltage, drawing energy from the power supply. The designer at the technology and architectural level can try to minimize the variables in this equation to minimize the overall energy consumption. However, minimizing power consumption is often a complex process of tradeoffs between speed, area and power consumption. Static power consumption is caused by short circuit currents, bias and leakage currents. At the time of change on the input of a CMOS gate, p and n channel devices may conduct simultaneously, briefly establishing a short from the supply voltage to ground. While statically biased gates are usually found in a few specialized circuits such as PLAs and their use has been drastically reduced. Leakage current is becoming the dominant component of static power consumption. Beforehand it was seen as a secondary order effect however, the total amount of static power consumption doubles with every new process node. Energy consumption in CMOS circuitry is proportional to the capacitive effect therefore a technique that can be used to reduce energy consumption is to minimize the capacitance. This goal is achieved at the architectural level of design as well as at the logic and physical implementation level. Interconnections to external components, such as external memory will typically have much greater capacitance than connections to on chip resources. Hence, accessing external memory can increase energy consumption. Otherwise, a way to reduce capacitance is to reduce external access and optimize the system by using on chip resources such as caches and registers. In addition, use of fewer external outputs and infrequent witching will result in dynamic power savings. Routing of capacitance is the main cause of the limitation in clock frequency. Circuits that are able to run faster can do so as a lower routing capacitance thereby dissipating less power at a given clock frequency. So energy reduction can be achieved by optimizing the clock frequency of the design, even if the resulting performance is fair in excess of the requirements.

POWER REDUCTION TECHNIQUES

The most effective and optimized ways of reducing power at the technological level is to reduce the supply voltage, because the power consumption drops quadratically with the supply voltage. But on the other hand lowering supply voltage may results in reduction of performance; therefore, any such voltage reduction must be balanced against any performance drop. To obtain and maintain the same throughput, extra hardware can be added.

ALTERNATIVE APPROACHES

The alternative approaches for reducing power consuming activity is by applying an asynchronous design methodology. CMOS is mostly used technology for low-power as gates only dissipate energy when they are switching. However, many gates will switch because they are connected to the clock, not because they have new inputs to process. Hence, a synchronous circuit wastes power when particular blocks of logic are not utilized.

TABLE 1. COMPARISON BETWEEN DIFFERENT ADDERS

DIFFERENT ADDERS	NO:OF MACROCELLS USED	AREA
Carry Look ahead Adder	9	68.300ns
Carry Select Adder	9	41.900ns
Ripple Carry Adder	8	42.900ns
Kogge-Stone Adder	6	28.700 ns

CONCLUSION

In microelectronics growing complexity and increasing operating clock frequencies have limited the scaling of process geometries and supply voltages thus producing an progressive rise in power dissipation. In current scenario power management at system level has become more important in the semiconductor industry and system developers are now looking for a wide range of semiconductor IP platform solutions that will eradicate the gaps between low-power and high-performance requirements. In this paper, a comparative study between different adders is done and various approaches for power reduction are also discussed for optimization so that tradeoffs between various adders for different applications are identified.

REFERENCES

[1] K. Sakthidasan, B.V Santhosh Krishna, "A New Chaotic Key Based Design for Image Encryption and Decryption of Digital Color Images", International Journal of Information and Education Technology, Vol.1, No.2, June 2011.

[2] Ambika Oad, Himanshu Yadav, Anurag Jain "A Review: Image Encryption techniques and its terminologies", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-3, Issue-4, April 2014.

[3] Rithmi Mitter, M.Sridevi Sathya Priya, "A Non Linear Equation Based Cryptosystem for Image Encryption and Decryption", 2012. International Conference on Computing, Electronics and Electrical Technologies [ICCEET]

[4] K.Dheergha Rao and Ch.Gangadhar,"Modified Chaotic Key Based Algorithm for Image Encryption and its VLSI Realization,"IEEE International conference on Digital Signal Processing (DSP-2007),July1- 4,2007,Cardiff,Wales,U.K, pp.439-442.

[5] K Dheerga Rao, K. Praveen Kumar, and P.V Muralikrishna, "A New and Secure Cryptosystem for Image Encryption and Decryption" appear in IETE Journal of Research, March April 2011.