Improved Security in Multi AESTHETIC Processor using AES Architecture

V.SrirengaNachiyar
PG scholar
Department of Information Technology
National Engineering College

R.Dhaya
Assistant Professor
Department of Information Technology
National Engineering College

ABSTRACT
Cryptography is the science of writing in secret code and is an ancient art. Cryptography not only protects data from theft or alteration, but can also be used for user authentication. In cryptography, encryption is the conversion of data into a form called a cipher text that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood. Cryptographic algorithms are at the heart of secure systems worldwide, providing encryption for millions of sensitive financial government & private transactions daily. In "AESTHETIC Processors Using AES Architecture for Flexible Security ", AES algorithm can be used for high speed and for high throughput. AESTHETIC processor supports original algorithm and also provides flexibility to configure the parameters of each of four transforms defined in AES algorithm. In this project it is proposed to develop a multiple AESTHETIC processor to achieve high speed and enhance the security level. The architecture performs encryption and decryption of large data with 128-bit key in CBC mode using on-the-fly key generation & composite field S-Box.

Keywords
AESTHETIC Processor, AES Algorithm, Cryptography, CBC mode

1. INTRODUCTION
Application such as electronic transaction and smart cards require not only significant network bandwidth but also high security measures[1],[2]. Powerful security processing architectures are thus important in high-speed network application. Today AES algorithm is used in a wide range of application in internet and wireless communication. In the project, the design of AESTHETIC (Advanced Encryption Standard with Tsing Hua ExTended and Implicit Configurability), an AES processor. The encryption and decryption procedures are architecturally the same as AES algorithm, however the data is manipulated in a different way, since the parameters are changed on-the-fly key generators have been used to generate the round keys concurrently during the encryption and decryption procedure without extra memory to store the sub-keys [7]. In the security processing architecture, use multiple AESTHETIC processor to achieve high speed and enhance the security level. Independent data path for each encryption block (input/output (I/O) first-in first-out and the AESTHETIC processor) ensures high-speed data encryption [1], [7].

2. RELATED WORK
P. Chodowiec, P. Khuon, and K. Gaj proposed the pipelining technique used to speed up the operation of digital systems by processing multiple blocks of data at the same time. The goal of pipelining stages is first to obtain the architecture with optimum throughput to area ratio and the architecture with highest possible throughput. Pipelining is used to speedup the operation of digital systems by processing multiple blocks of data at the same time. New methodology called mixed inner- & outer-round pipelining offers high throughput, small area and achieves high speed up. [3].

S. Mansards, M. Aigner, and S. Dominikus proposed a highly regular and scalable AES hardware architecture, suited for full-custom as well as for semicustom design flows. Contrary to other publications, a complete architecture that is scalable in terms of throughput and in terms of the used key size is described. Applications with strict requirements concerning performance, power consumption, or side-channel leakage are, in practice, usually implemented by dedicated hardware. Hardware implementations of the AES are, for example, used in Internet servers as performance accelerators or in smart cards (besides other reasons) to increase the resistance against side-channel attacks.[4]

J. H. Shim, D. W. Kim, Y. K. Kang, T. W. Kwon, and J. R. Choi implemented a cryptoprocessor using a shared on-the-fly key scheduler which performs forward key scheduling for encryption and reverse key scheduling for decryption. The encryption and decryption share the same key scheduler. Generally, Rijndael has been implemented in software, but a software implementation cannot offer the physical security for the key. Rijndael is implemented in hardware with on-the-fly key scheduler, which can make not only a forward scheduling for encryption but also a reverse scheduling for decryption. Therefore. it enhances the physical security and an outside attacker cannot easily modify it.[5]

3. PROPOSED METHODOLOGY
3.1 Input/Output Block Converter:
Whenever the encryption or decryption procedure is enabled by the main controller, the input data block will be retrieved from the input buffer and converted to the composite field representation in the input block converter [3]. This converter provides the following functions

a) Mapping the initial key
b) Mapping the sum of input data block
c) Mapping the input data block in the ECB mode.

3.2 Main controller:

The main controller controls the AESTHETIC engine, the key generator, and the I/O interface. The AESTHETIC data path will write the encrypted/decrypted data to the output buffer [3].

3.3 AESTHETIC engine:

AESTHETIC engine consists of four transform in the extended AES algorithm and is used for both encryption and decryption. The block S-Box implements the transform for a 128-bit data block. ShiftRows and InvShiftRows perform the same functions as defined in the original algorithm. Since operations are done byte-wise, it makes no difference [1]. The MixColumn and InvMixColumn functions can easily run on the same hardware by changing the co-efficients according to the processing mode. The host processor controls each AESTHETIC processor via an AHB like interface [2]. First, when the host processor has to perform a security processing task, it checks which AESTHETIC processor is free with the resource control register of the shared module. If one or more AESTHETIC processor are available, it sets the corresponding bits of the register for the selected AESTHETIC processor. Otherwise it waits. The figure2 shows three AESTHETIC architecture [1] .

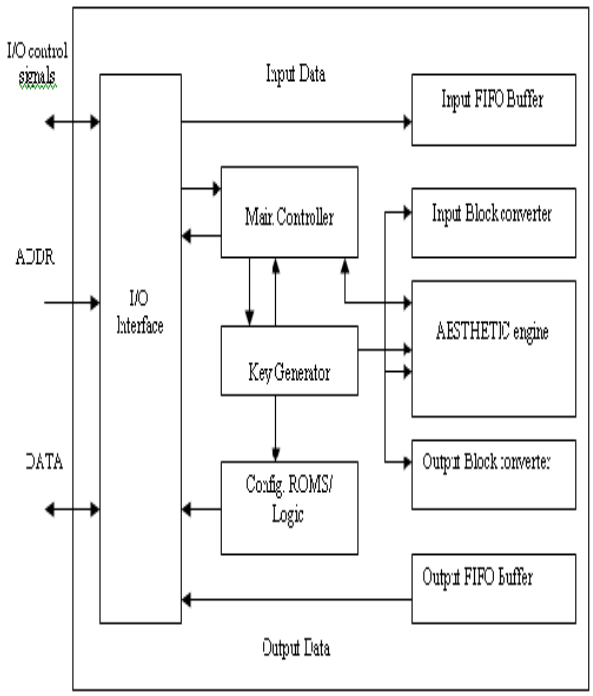

Figure 1: Single AESTHETIC processor

The data access can be carried out simultaneously with 128-bit block encryption as well.The main controller issues an interrupt to the host processor after an encryption task is complete. In the multi-core architecture the critical path lies in AESTHETIC engine, not the control path.

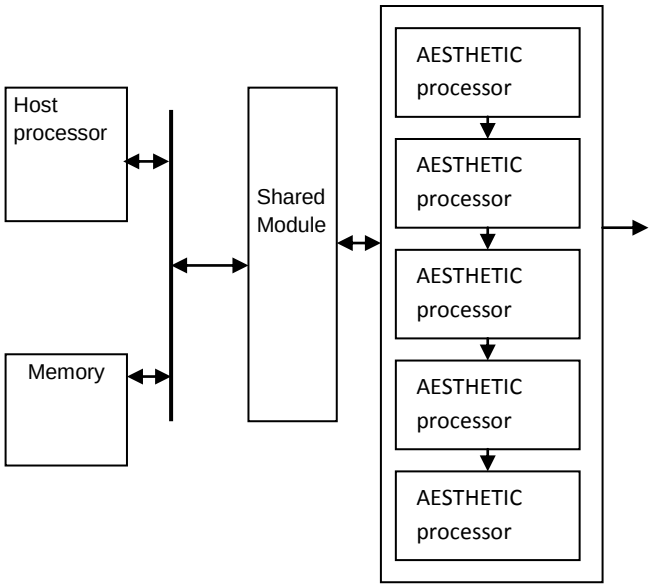

Figure 2: Five AESTHETIC processor

The multi AESTHETIC architecture gives high throughput and it enhances the security. Using independent data path, it ensures the high speed data encryption and decryption [1].

3.3.1 Encryption:

In cryptography, Encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information in cryptography, referred to as cipher text [2],[7].

3.3.1.1 SubBytes:

In the SubBytes step, each byte in the matrix is updated using an 8-bit substitution box, the Rijndael S-box. This operation provides the non-linearity in the cipher. The S-box used is derived from the multiplicative inverse over GF (2^8), known to have good non-linearity properties [2], [7].

3.3.1.2 ShiftRows:

The ShiftRows step operates on the rows of the state; it cyclically shifts the bytes in each row by a certain offset. For AES, the first row is left unchanged. Each byte of the second row is shifted one to the left. Similarly, the third and fourth rows are shifted by offsets of two and three respectively. For the block of size 128 bits and 192 bits the shifting pattern is the same [2].

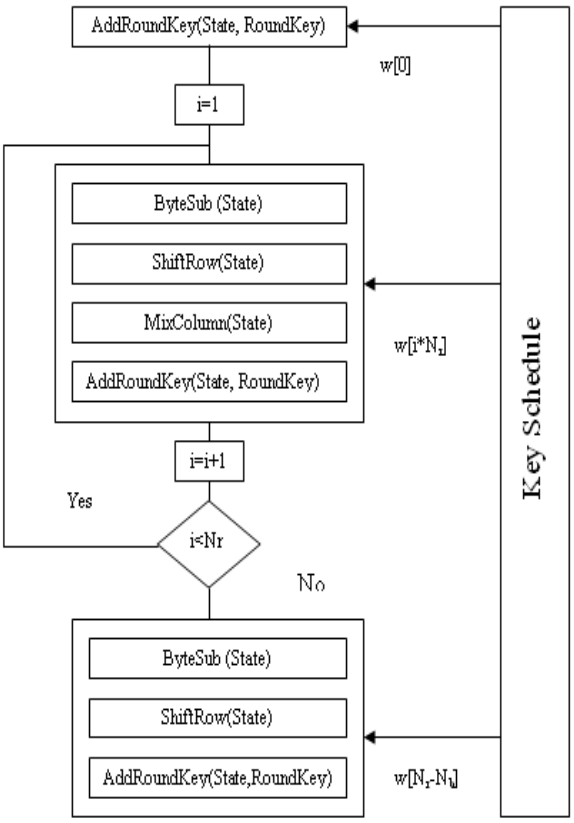

Figure 3: Encryption process

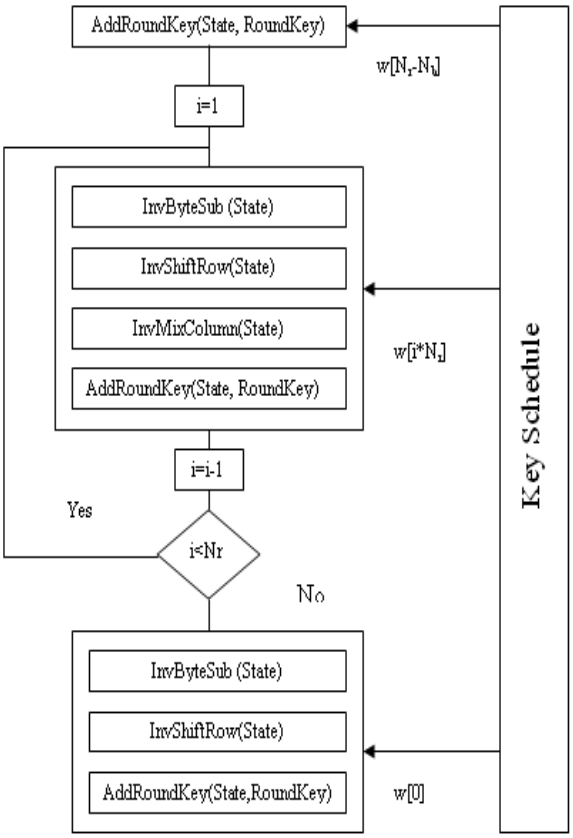

Figure 4: Decryption process

3.3.1.3 MixColumns:

In the `MixColumns` step, the four bytes of each column of the state are combined using an invertible linear transformation. The `MixColumns` function takes four bytes as input and outputs four bytes, where each input byte affects all four output bytes.[2].

3.3.1.4 AddRoundKey:

In the `AddRoundKey` step, the subkey is combined with the state. For each round, a subkey is derived from the main key using Rijndael's key schedule; each subkey is the same size as the state. The subkey is added by combining each byte of the state with the corresponding byte of the subkey using bitwise XOR [2].

3.3.2 Decryption:

The decryption process is direct inverse of the Encryption process. All the transformations applied in Encryption process are inversely applied to this process. Hence the last round values of both the data and key are first round inputs for the Decryption process and follows in decreasing order. The above figure shows the process of decryption. Four steps in decryption process are

1) InvSub Bytes
2) InvShift Rows
3) InvMix Column

4. PERFORMANCE EVALUATION AND RESULTS

The AESTHETIC processor using AES algorithm was implemented on xilinx virtex-II platform. The minimum period required for three AESTHETIC processor is 32.296ns in 30.640MHz frequency. The minimum period required for five AESTHETIC processor is 32.971ns in 30.330MHz frequency. The consumption of slices and flip-flops was estimated using Xilinx.

The number of slices and the number of flip-flops consumed by the three AESTHETIC processor are 504 and 445. The number of slices and the number of flip-flops consumed by five AESTHETIC processor are 521 and 391. The comparison between three and five AESTHETIC processor as shown in Table 4.1.

Table 1. Performance Evaluation

No. of processor	Time period (ns)	No. of slices	No. of flip-flops	Freq. (MHz)
Three	32.579	499	448	30.695
Five	32.971	451	359	30.330

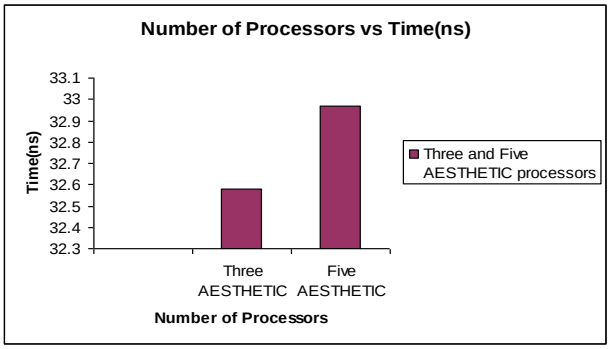

Figure 5: Number of Processors vs Time (ns)

The figure 5 shows the time comparison between the three and five AESTHETIC processors. Even though the number of processor increased, the time requirements and also the consumption of slices and the flip-flops is not so much differed between three and five AESTHETIC processor.

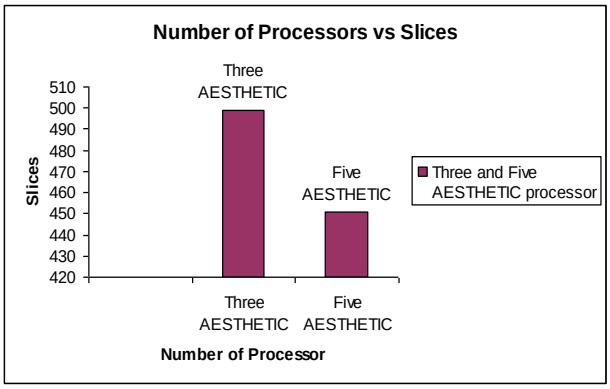

Figure 6: Number of Processors vs Slices

The figure 6 shows the number of slices occupied by the three and five AESTHETIC processors. There is no much difference in the slices occupied by three and five AESTHETIC processors

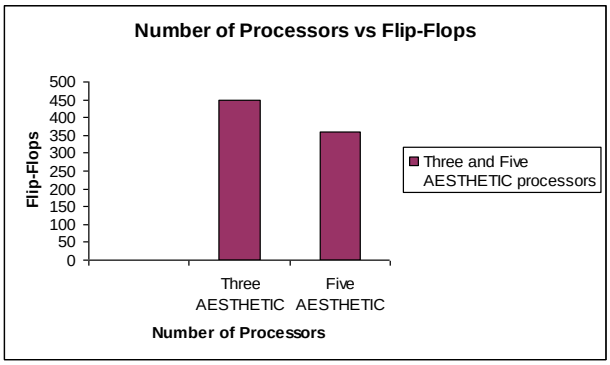

Figure 7: Number of Processors vs Flip-Flops

The figure 7 shows the Number of Flip-Flops occupied by the three and five AESTHETIC processors.

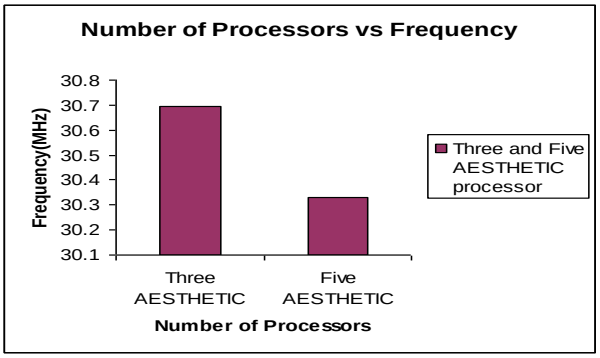

Figure 8: Number of Processors vs Frequency (MHz)

The figure 8 shows the Maximum operated Frequency by the three and five AESTHETIC processors. The below fig: 9 shows the results of single AESTHETIC processor.

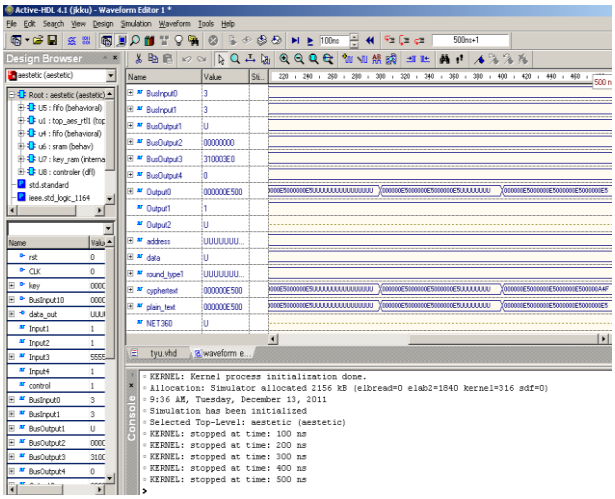

Figure 9: Single AESTHETIC processor

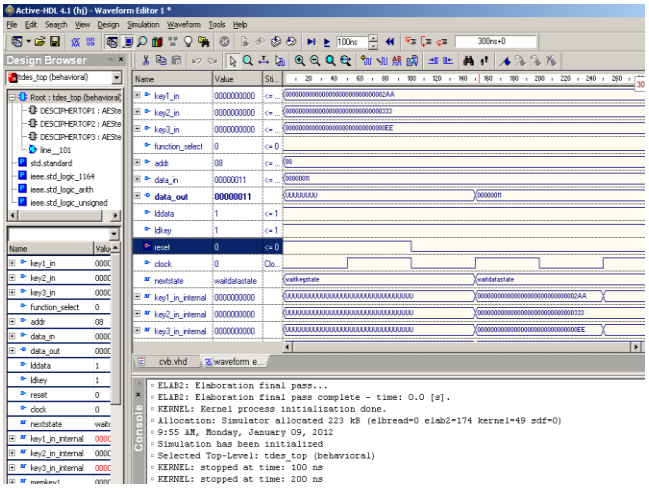

Figure 10: Three AESTHETIC processors

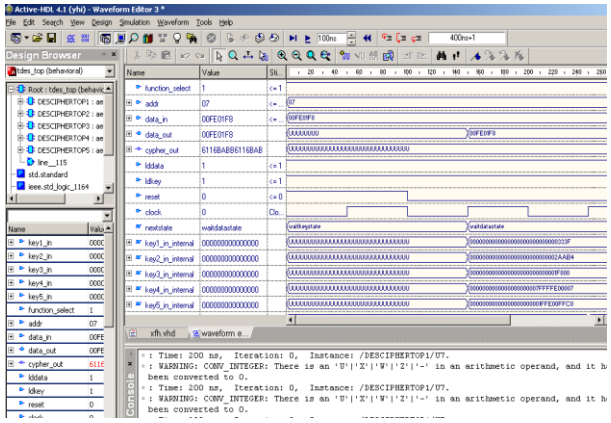

Figure 11: Five AESTHETIC Processors

The above (figure 10, figure 11) shows the results of three AESTHETIC and five AESTHETIC processors.

5. CONCLUSION

A configurable AES chip, called AESTHETIC, which enhances security over standard AES designs. The chip supports ECB and CBC cipher modes with 128-b keys. It can be used in not only the extended AES algorithm but also the original AES algorithm. Based on our AESTHETIC processor (with configurable S-box and MixColumns transforms), we also propose a high-performance multicore architecture, where independent data path for each AESTHETIC processor provides multigigabit security processing without I/O bandwidth problem. The memory controller coordinates the maximum overlapping between data transfer and encryption (decryption) process.

6. REFERENCES

[1] Mao-Yin Wang, Chih-Pin Su, Chia-Lung Horng,cheng Wen Wu, and Chih-Tsun Huang, "Single- and Multi-core Configurable AES Architectures for Flexible Security. IEEE Transactions on Very Large Scale Integration (VLSI) Systems. 2010, pp 541-552.

[2] C.-P. Su, C.-L. Horng, C.-T. Huang, and C.-W. Wu, "A configurable AES processor for enhanced security," in Proceedings ASP-DAC, 2005, pp. 361–366.

[3] E.J. Swankoski, R. R. Brooks, V. Narayanan, M.Kandemir, and M. J. Irwin, "A parallel architecture for secure FPGA symmetric encryption," in Proceedings 18th International. Parallel Distribution Processing Symposium, Santa Fe, NM, . 2004, p. 132.

[4] S. Mangard, M. Aigner, and S. Dominikus, "A highly regular and scalable AES hardware architecture," IEEE Transaction on Computers, 2003. pp. 483–491.

[5] J. H. Shim, D. W. Kim, Y. K. Kang, T. W. Kwon, and J. R. Choi, "A rijndael cryptoprocessor using shared on-the-fly key scheduler," in Proc. 3rd IEEE Asia-Pacific Conference ASIC, Taipei, Taiwan, Aug. 2002, pp. 89–92.

[6] S. Morioka and A. Satoh, "A 10 Gbps full-AES crypto design with a twisted-BDD S-Box architecture," in Proceedings. IEEE ICCD, 2002, pp. 98–103

[7] J. Wolkerstorfer, E. Oswald, and M. Lamberger, "An ASIC implementation of the AES S-Boxes," in CT-RSA 2002., pp. 67–78.

[8] National Institute of Standards and Technology, Springfield, VA, "Advanced Encryption Standard (AES)," Nov. 2001.

[9] P. Chodowiec, P. Khuon, and K. Gaj, "Fast implementations of secret key block ciphers using mixed inner- and outer-round pipelining," in Proceedings International Symposium Field Programmable Gate Arrays, Monterey, CA, 2001, pp. 94–102

[10] V. Fischer and M. Drutarovsky, "Two methods of Rijndael implementation in reconfigurable hardware," in Cryptographic Hardware and Embedded Systems (CHES), 2001, pp. 77–92.