Survey on FPGA-based Pipelined Architecture for RC5 Encryption

Ashmi Singh
NRI Institute of Information Science & Technology bpl

Puran Gour
NRI Institute of Information Science & Technology bpl

Brij Bihari Soni
NRI Institute of Information Science & Technology bpl

ABSTRACT
In current scenario, electronic devices handling confidential information. In these devices encryption algorithm proposed have been satisfy to protect the confidential information and known for their cryptographic applications. The extensively use of reconfigurable processor like FPGA for cryptographic application which have reduced the time to market of hardware logic. In this survey presented that the FPGA-based hardware architecture is best approach for high performance of circuit, it reduces the response time and resources. This hardware architecture work on Verilog as well as VHDL language.

Keywords: FPGA, RC5, Pipeline.

1. INTRODUCTION
Security of the data is important for applications that need privacy like military and defense etc. To fulfill this purpose, we need cryptographic algorithms.

Cryptographic algorithms are used to ensure the privacy of data by providing required security through encryption. In cryptography process, plain text is converted in cipher text at the transmitter side and again converted in Plain text at the receiver side. Encryption is carried out by performing complex mathematical operation on the data using secret key, and this complex operation require extra power , time and resources. Encryption algorithm are of two types, stream and block cipher. In cryptography a block cipher is a deterministic algorithm operating on fixed-length groups of bits, called blocks, with an unvarying transformation that is specified by a symmetric key. RC5 cryptography algorithm is symmetric key block encryption which operates on w-wide bit data for r-round using b-bytes of key to add to flexibility. It is simple algorithm uses round wise data dependent. For RC5 cryptography and its implementation proposed a dedicated hardware [1] .In this proposed hardware, are introducing a new hardware-oriental algorithm into the shift round process during encryption and decryption, high-speed processing and area reduction were realized.

Desisn a new architecture for RC5 algorithm in FPGA which reduces the waiting time by data schedule using the sliding window method[4].

In this paper for high performance presented survey & comparison on "FPGA based pipelined Architecture for RC5 Encryption algorithm "which Improves the response time of the system with less resources, and performance of this architecture provide the high throughput.[5] The drawback of this architecture is, since only one key is use the encrypt the data; it is easy to retrieve the intermediate result of any round through the pipeline.

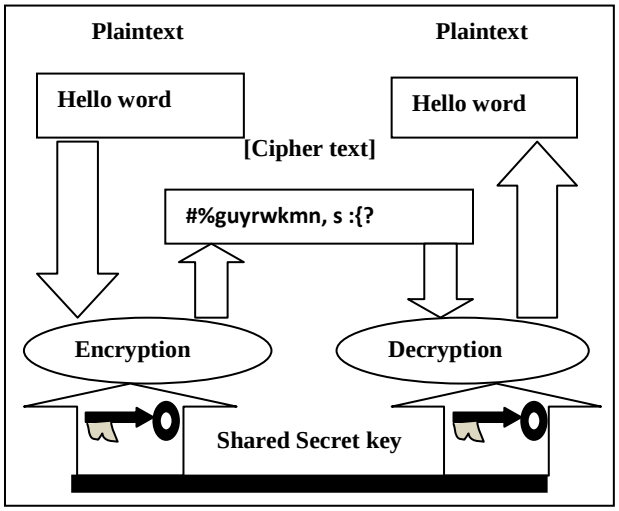

Fig 1: Cryptography

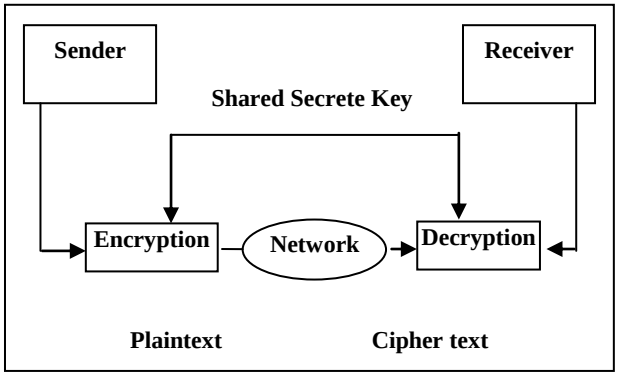

Fig 2: Symmetric key cryptography

2. LITERATURE REVIEW

Table 1: Comparison among noted papers

Parameters	Paper I	Paper II	Paper III	Paper IV	Paper V
Name	FPGA based Pipeline-d Architecture for RC5 Encrypt-ion.	FPGA based Sliding Window Architect-ure for RC5 Encrypti-on.	A Pipeline VLSI Architect u-re for Fast Comput-ation of the 2-D DWT.	Pipelined Architecture for FPGA Implementation of Lifting-Based DWT.	Dedicated hardware for RC5 cryptography and its Implementation.
Author	A.Ruhan Bevi, & S.S.V.Sheshu	A.Ruhan Bevi, & S.S.V.S Heshu	Chengj-un Zhang& Chunyan Wang	ZhiWei WU & Wei WANG	Masay-a yoshikawa & Koichi Sakau-e
Year	2012	2012	2012	2011	2011
Publication	IEEE	ICACCI	IEEE	IEEE	-
FPGA	Xilinx Vertex-II Pro.	Xilinx	XC2V250,	Altera	XC5VLX30/50
Tools Used	Xilinx Vertex-II Pro	VHDL	XC2V250	Altera	Verilog HDL
Operating Frequency	116 MHz	104 MHz	153 MHz	68.33 and 96.64 MHz	N/a
Work	Using H/CDFG Model was design pipelined architecture for RC5 which improves response time of the system	Using Slinding window method was design FPGA based architecture which reduces waiting time by sehedule.	Using 2-D DWT was design 3-stage pipeline architecture for a real time computation of 2-D DWT .	Using lifting scheme with DWT algorithm was design architecture for speedin up performance.	RC5 Dedicated hardware by introducing an architecture suitable for each operation used for the encryption.

FPGA based pipelined Architecture fort RC5 Encryption many work have been done which are as follow-

In 2011's, Masaya & Sokaun proposed RC5 Dedicated hardware, by introducing an architecture suitable for each operation used for the encryption[1]. RC5 is a common key block cipher in which the size of the block, the no of the rounds and size of key can be changed. In proposed architecture the high speed processing and area reduction are introduces by arithmetic processes which suitable for hardware during encryption and decryption. Thus this hardware has been given better high speed process and area reduction can be realized.

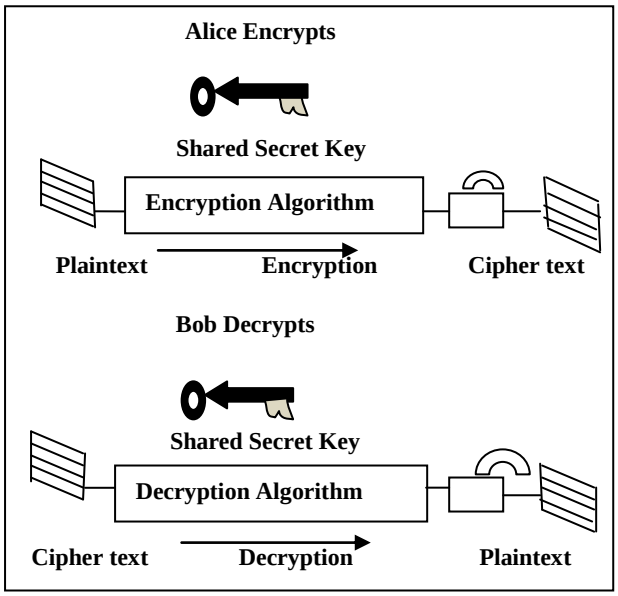

Fig 3: Encryption and Decryption with symmetric key

Zhigang & Wang (2011) presented high speed 9/7 lifting 1D-DWT algorithm which is implementation of FPGA with multistage pipelining structure for speeding up performance [2]. The main feature of the lifting based discrete wavelet transform scheme is to break up the high pass and low pass wavelet filters into a sequence of smaller filters.

The lifting algorithm can be computed in three phase in equation which are as follows-

1. Split Phase

Xe =X (2n), Xo=X (2N+1)

2. Prediction Phase

Y (2N+1) =Xo (2n+1)-P (Xe)

3. Update phase

Y (2n) =Y (2n+1) +U (Xe)

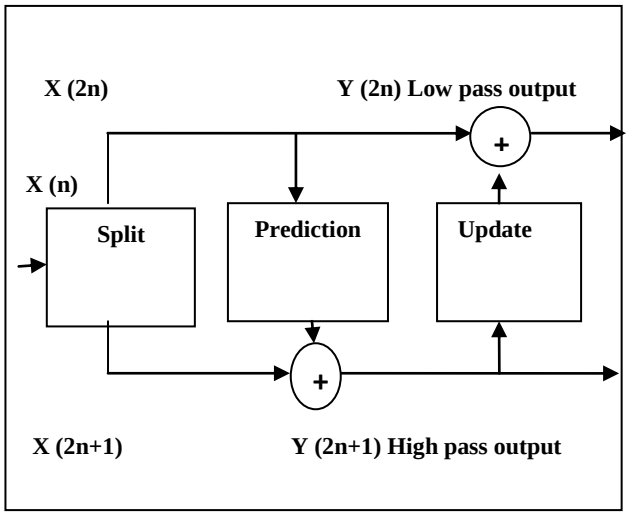

Fig 4: Split, predict and update phases of the lifting based DWT

In 2012, Chengjun et.al(2012) proposed "A pipelined VLSI Architecture for fast computation of the 2-D Discrete Wavelet Transform".[3] In this paper authors presented 3- stage pipeline architecture for real time computation of 2-D DWT. The objective has been to achieve a short computation time by maximizing the clock frequency (1/Tc) required for the DWT computation by developing a scheme for enhanced inter-stage and intra-stage computation. This approach given fast computation for 2D-DWT with low cost on based on FPGA.

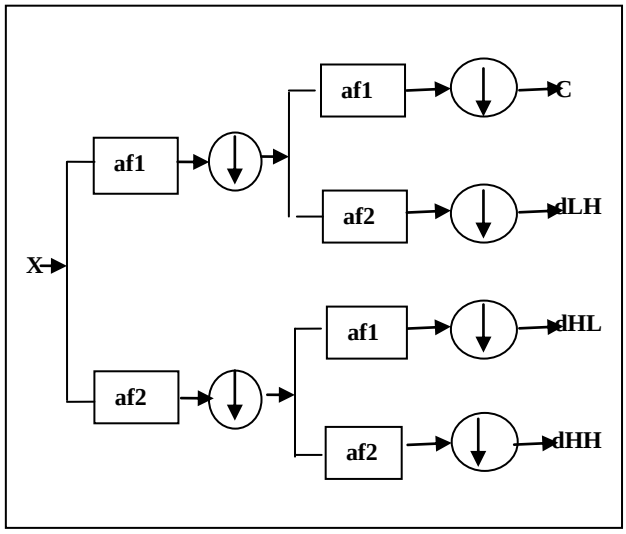

Fig5: 2D-Discrete Wavelet Transfrom.

In 2012, Ruhan Bevil et al. presented FPGA based Sliding Window Architecture for RC5 Encryption which reduces the waiting time by schedule using sliding window method [4].
The sliding window is a popular data link layer protocol widely used in data transmission methods and this architecture used in busy data traffic network. The proposed design is implemented on Xilinx FPGA Vertex- II. FPGA is a reconfigurable device, so it reduces the time of this proposed architecture. The future scope of this work will be where priority of the data has a given more emphasis with sliding window.
Ruhan Bevil et al.(2012) again presented FPGA based pipelined architecture for RC5 that improves response time of the system with less resources using H/CDFG technique[5]. H/CDFG is made of combination of different CDFG's and DFG's which describes the data flow and control transfer in the design, often used in many design approaches to reduce time to design .The proposed hardware implementation is more suitable for RC5 as it is achieve to response time and high throughput result will term on both of speed and security.
The works similar to the objective extend plateform understand the design problems published by many workers. [6],[7],[8],[9],[10],[11],[12],[13],[14],[15] & [16].

3. PROBLEM FORMULATION

In 2011, Problem are solved by new hardware oriented algorithm into shifted arithmetic, mixture ,and round processes during encryption and decryption ,high speed processing and area reduction were realized .this proposed architecture incorporate it into on FPGA. FPGA used in experiment was SASBEBO-GII (XC5VLX30/50) and design is handling by verilog HDL.
In 2011, problem is formulated by discrete wavelet transform algorithm based architecture which is used to multistage pipeline for the proposed speeding up the performances. Design were implemented and simulated on Stratix FPGA device from Altera is delivers highest density, highest performance and lower power which provide superior signal integrity.

Fig 5: Stratix-IV FPGA Altera

In 2012, problem is formulated by 3-stage structure for computation of 2D-DWT.The operation of the 3-stage need to be synchronized in a manner so that three stages perform the computation of multiple decomposition levels within a minimum possible time period. Thus proposed design implementations are more suitable on FPGA as it given the best performance.
In 2012, problem are overcome by sliding window technique which is used design hardware architecture and this hardware architecture perform in Xilinx FPGA which provide faster encryption and reduced the waiting time. Implementation are perform in FPGA vertex pro II and design is handle by VHDL.

In 2012, problem is solved by H/CDFG technique .this technique is used in many design approaches to reduces time of design. FPGA are reduces the time of design as it is this proposed scheme are reduce the response time and less resource in FPGA which provide high throughput.

Table 2: FPGA implementation results of four papers

Architecture	Slices	Delay	Frequency (MHz)
A.Ruhan Bevi[5]	1698	8.62	116
A.Ruhan Bevi[4]	1406	9.390	104
M.Yoshikawa[11]	2488	9.920	100
C.Zhang[3]	2842	N/A	135

4. RESEARCH OBJECTIVE

The main objective of this research reduced the increased response time of overall system and resources. In earlier days, when we design Pipelined architecture without RC5, in this case many rounds and extra time is needed so that it becomes very difficult to design. After that we use new high performance pipelined Architecture for RC5, this architecture design is provide a best performance and reduced the increased response time and resources in FPGA with high throughput that's why we used FPGA based pipelined Architecture for RC5 Encryption.

FPGA is an integrated circuit designed to be configured by a customer or a designer after manufacturing – hence this is field programmable. The FPGA configuration is generally specified using a hardware description language(HDL).

From above, we can say that FPGA play widespread role. FPGA is reconfigurable processors extensively used for cryptography application which have reduced the time of overall system. Thus we can use FPGA for best results.

6. CONCLUSION AND FUTURE SCOPE

We conclude from this survey FPGA based pipelined Architecture is better than Software based pipelined Architecture. It is best approach to reduce the response time and resources in few times and provide the best performance. The performance of the proposed architecture provides a high throughput of 6.9 Gbps with 12-stage pipeline. This proposed architecture work on verilog as well as VHDL language.

In contrast Software based hardware architecture more time taken reduces the response time of design. Thus this approach are not better than FPGA based pipelined architecture.

7. REFERENCES

[1] Masaya Y., and K. Sakaun 2011. "Dedicated hardware for RC5 cryptography and its Implementation".

[2] Zhigang wu and Wei wang, 2011. "Pipelined Architecture for FPGA Implementation of Lifting-Based DWT".

[3] Chengjun Z. Chuyan W., and M. omair Ahmad, 2012. "A Pipeline VLSI Architecture for Fast Computation of the 2-D Discrete Wavelet Transform".

[4] A. Ruhan Bevi1, S.S.V. Sheshu, and S. Malarvizhi"2012. FPGA based Sliding Window Architecture for RC5 Encryption".

[5] A. Ruhan Bevi1, S.S.V. Sheshu, and S. Malarvizhi 2012. "FPGA based Pipelined Architecture for RC5 Encryption".

[6] K El-latif, 2010. "Hardware Implemented of DES using Pipelining Concept with Time-Variable Key". 22nd International Conference on Microelectronics (ICM), Egypt.

[7] A.Klimm, M.Haas, O.Sander, and J.Becker, 2010. "A flexible integrated crypto processor for authentication protocols based on hyper elliptic curve cryptography", Proc. of International Symposium on System on Chip (SoC), pp.35-42,

[8] A.Irwansyah, V.P.Nambiar, and M.Khalil-Hani 2009. "An AES Tightly Coupled Hardware Accelerator in an FPGA-based Embedded Processor Core".pp.521-525

[9] B.B.Brumley, and K.U.Jarvinen, 2010."Conversion Algorithms and Implementations for Koblitz Curve Cryptography".pp.81-92

[10] M.Rahman, I.R. and Rokon, 2009. "Efficient hardware implementation of RSA cryptography", Proc. of International Conference on Anti-counterfeiting, Security, and Identification in Communication, pp.316-319.

[11] F.A.G.Muzzi, R.B.Chiaramonte, and E.D.M.Ordonez, 2009. "The Hardware-based PKCS#11 Standard using the RSA Algorithm", pp.160-169.

[12] Zhang Lina, 2010. "Research on critical technology of elliptic curve cryptosystem SOC". Proc. of International Conference on Communication Systems, Networks and Applications. pp.77.80.

[13] Zhimin Chen, P.Schaumont, "Early feedback on side channel risks with accelerated toggle-counting", Proc .of IEEE International Workshop on Hardware-Oriented Security and Trust, pp.90-95.

[14] Juha Kukkurainen, Mikael Soini, and Lauri Sydanheimo, 2010. "RC5-Based Security in Wireless Sensor Networks: Utilization and Performance".

[15] Yain-Reu Lin; Chia-Hao Hsu; Rieger, and R.; Chua-Chin Wang, "Low power RC5 cipher for ZigBee portable biomedical systems", pp 615 – 616.

[16] Dhanashri H. Gawali and Vijay M. Wadhai, 2012. "RC5 algorithm: potential cipher solution for security in wireless body sensor networks"