ISSN 2278-5612

A Review Paper on Comparative Study of FPGA Implementation of Adhoc Security Algorithms

Dr. Seema Verma[1], Pooja Srivastava[2], Divya Ramavat[3], Nupur Srivastava[4]

[1]Assosiate Professor, Department of Electronics, Banasthali University, India
seemaverma3@yahoo.com
[2]Assistant Professor, Department of Electronics, Banasthali University, India
pooja_enn@yahoo.co.in
[3]Student, M.Tech (VLSI Design), Banasthali University, India
divyaramavat@gmail.com
[4]Student, M.Tech (VLSI Design), Banasthali University, India
nupur.srivastava13@gmail.com

ABSTRACT

Nowadays data security is an important issue for decentralized networks like Adhoc Network. In this paper, we have proposed the study of five FPGA implementated data security algorithms specially designed for adhoc network. We have proposed the role of FPGAs within a security system and provided the solutions to security challenges. The result shows that FPGA implementation outperforms software and processors implementation by 20 and 140 times respectively.

Indexing terms/Keywords

Adhoc Networks, FPGA, Mannets,VHDL

Academic Discipline And Sub-Disciplines

Wireless Communication, VLSI Design

SUBJECT CLASSIFICATION

Security Studies

TYPE (METHOD/APPROACH)

Conceptual Paper

Council for Innovative Research
Peer Review Research Publishing System
Journal: International Journal of Management & Information Technology

Vol. 7, No. 1
editor@cirworld.com
www.cirworld.com, member.cirworld.com

ISSN 2278-5612

INTRODUCTION

In todays scenario, telecommunication technologies are advanced to provide networking facilities even in remote areas where predesign network infrastructure is not available. A decentralized node network where a number of nodes can communicate with each other anytime and anywhere called Adhoc network, which is applicable in such fields. Mobile ad hoc networks (MANETs) are a collection of wireless hosts that communicate with each other through multi-hop wireless links, without the existence of any infrastructure or administrative authority. Therefore nodes must collaborate between them to accomplish some operations like routing and security. Adhoc networks have wide applications in professional, military, and rescue operation fields where it is required to share data efficiently and fastly without any infrastructure assistance [1]-[5].

As we have seen above that Adhoc network is being used for defence and rescue operation fields, where the information being transmitted is highly confidential. Security of such information, is important and hence security is a main issue for adhoc networking. Wireless networks are more prone to security attacks as all transmissions are carried out using the air medium. They are especially susceptible to attacks of eavesdropping, replay and spoofing. These systems therefore need to have built-in features to withstand these attacks without compromising security in any way. The classification of security services in any network can be given as follows: Confidentiality, Encryption, Integrity, Access Control and Availability. While designing an adhoc network, security algorithms also need to be implemented to maintain the secracy of the data. Two kinds of security algorithms are designed for adhoc networks namely symmetric algorithms (conventional encryption) and asymmetric algorithms (public key encryption) [6]-[8].

For implementing the security algorithms upon practical system, three main approaches are followed eg: microprocessors, ASIC and FPGA implementations. In this paper, we are emphasizing upon FPGA technology. Security algorithm programs can be return in VHDL or Verilog environment and are downloaded to the FPGA chip. Most of this chip are in circuit programmable and hence the encryption key can be changed online. A gate array is a particular arrangement of transistors fabricated upon a single chip. Different arrangements of inter-connect metal layers can be added in order to define the function of the circuit. This allows that same mass produce wafers can be used for performing different logic functions. Field programmability is the property that allows the functionality of a device to be modified according to the program. FPGA circuits utilizing SRAM and EPROM programming technologies are volatile in nature that is same circuit can be modified according to different digital function. Device configuration can be programmed to be portable between miscellaneous FPGAs without any adaptation. FPGAs also provide extremely short time to market due to earlier availability of hardware prototypes. FPGA system works very efficiently as it is exactly customized for the designated task. High performance gain can be achieved by providing parallelization and customization for the specific task. FPGA technology provides real time deterministic behavior of the system. On the basis of these facts now it is clear that fabrication technology is being shifted from ASIC to FPGA [9]-[11].

FPGA IMPLEMENTATION OF RECENT ALGORITHMS

Clustering algorithm

Software implementation of clustering algorithms have been suffered from power limitations at the time of high traffic. This algorithm provides solution of that problem by hardware implementation of K-means algorithm which is based on cluster based traffic. The advance algorithms for clustering are *k*-means [12], Hierarchical Clustering [13], Self-Organizing Maps [14] and Principal Component Analysis [15]. The algorithm can be explained as follows: first it takes input as the number of clusters (*k*) then cluster centers will be created by the random data points. Second arithmetic mean of each cluster will be calculated Euclidean or Manhattan distance measure will be used [16].

Implemented results

Hardware implementation of this algorithm has been performed by The Xilinx ISE and VHDL language [16]. The clock frequency 40 MHZ has been used and 32 packets in 11.8 microseconds has been processed. The result shows that hardware implemented design is 300 times faster than software implemented design.

Scalable encryption algorithm

SEA is a scalable encryption algorithm is the best known hardware algorithm for embedded applications. Initially this was designed for soft ware implementations**.** SEA has proposed parametric block cipher for resource constrained systems. It has provided low cost and small size encryption/authentication routine17]-[19]. $SEA_{n,b}$ operates on various text, key and word sizes. It is based on a Feistel structure with a variable number of rounds, and is defined with respect to the following parameters:

- n: plaintext size, key size.
- b: processor (or word) size.
- $n_b = n_{2b}$: number of words per Feistel branch.
- n_r: number of block cipher rounds.

As only constraint, it is required that n is a multiple of 6b (see [1] for the details). For example, using an 8-bit processor, we can derive a 96-bit block ciphers, denoted as $SEA_{96,8}$.

Let x be a $n/2$ -bit vector. We consider two representations:

- Bit representation: $x_b = x(n/2 - 1) \ldots x(2)\ x(1)\ x(0)$.
- Word representation: $x_W = x_{nb-1}\ x_{nb-2} \ldots x_2\ x_1\ x_0$.

Implemented results

In this implementation, the generic VHDL coding has been provided for flexibility. The presented parametric architecture supports both encryption and decryption at a minimal cost. As we know that in VLSI design: less area, maximum efficiency, high speed, time to market and low power consumption are the key issues. In this aspect, SEA exhibits very small area utilization and it is best solution for embedded applications [20].

NTRU-based algorithm

The NTRU (Nth degree truncated polynomial ring) encrypt algorithm provides low power consumption and high efficiency for complex security algorithms. Its public key cryptosystem is based on solution of lattice problems and concept of ring theory. It provides a ring R and two ideals p and q in R. Most of the computations are done on mod p or mod q, and all polynomials are taken modulo (XN_1). NTRU polynomial multiplier is used as star multiplication for multiplication in the ring [21]-[23]. Figure 1 shows the diagram of NTRU polynomial multiplier.

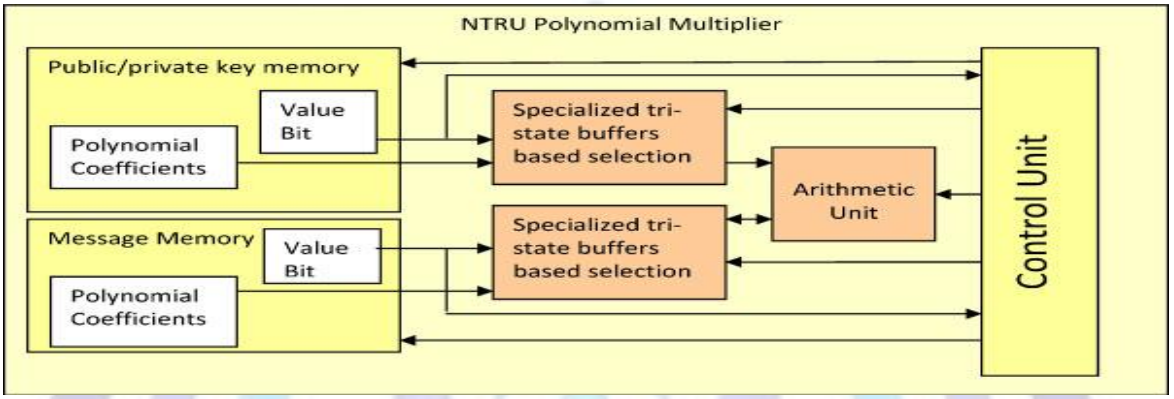

Fig 1: NTRU Polynomial Multiplier [24]

Implemented results

For hardware implementation, figure 2 has proposed the design procedure. The polynomial operands can be represented for chosen to maximize storage efficiency. By the help of minimization of number of gates, number of glitches and size of transistors, this algorithm has been reduced both static and dynamic power dissipation [24].

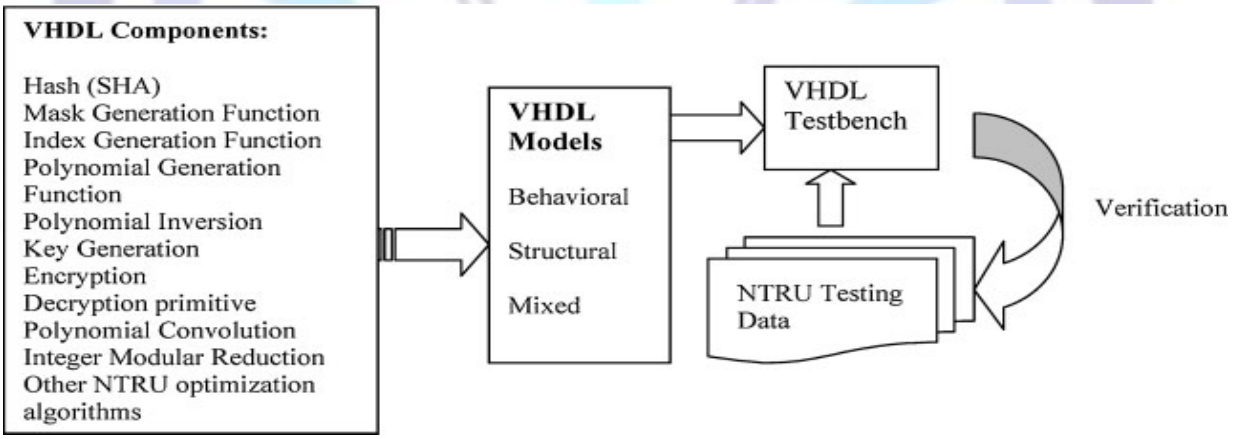

Fig 2: NTRU hardware design procedure [24]

Galois finite field algorithm

In this algorithm, network decoding scheme based on galois finite field operation has been described. The decoding mechanism needs higher complex mathematical operations as compared to encoding mechanism. Network coding is much more efficient than forward coding because multi cast process is completed in the single phase. Gaussian elimination and high probalitic algorithms is the heart of this prominent scheme. Encoding and decoding finite fields are divided in to prime fields and extension binary fields. For generation of the superior coefficient matrix, echeloning process has been used. Back substitution process has been dedicated for parallelism. The figure 3 has proposed the hardware implementation of decoding process.

Fig 3: Hardware implementation of decoding process[26]

Implemented results

VLSI implementation has been done by the help of VHDL (Very High Speed Hardware Description Language). The results has explained that there is the achievement of twice of the throughput due to the pipelining of echeloning and back substitution process [26].

HCgorilla double cipher algorithm

HCgorilla is the latest algorithm for reduced power dissipation in multimedia data. This hardware algorithm is based on the analysis of internal behaviour of processors. It is capable for bidirectional communication by the help of parallelism. This algorithm includes the following steps: Architecture level parallelism, Circuit module level, Instruction level parallelism and micro architecture level. HCgorilla has proposed for ubiquitous computing due to its functionality and usability. It has composed of 8 Java-compatible instructions with 2 SIMD mode cipher instructions. [27-29]. Figure 4 has been proposed the double cipher mechanism.

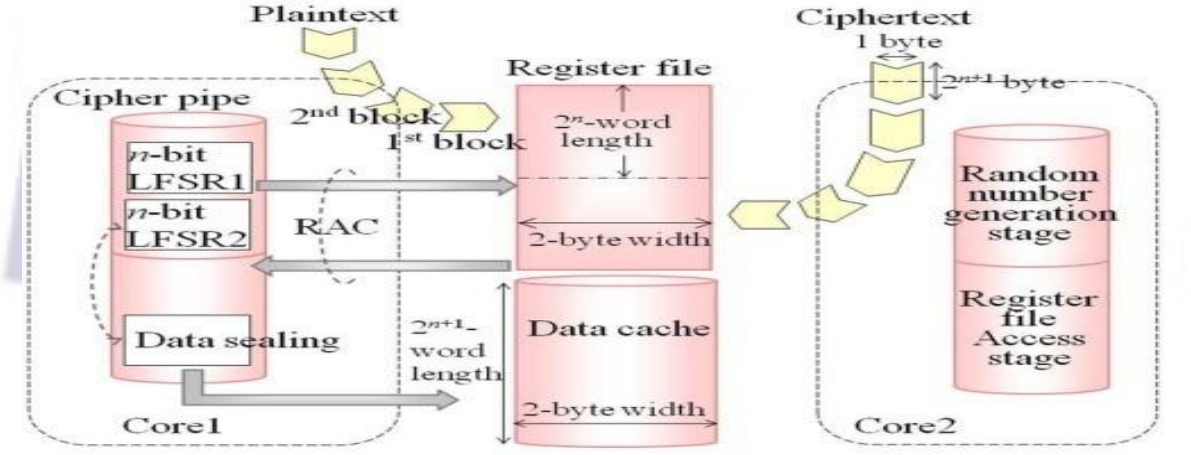

Fig 4: Double cipher mechanism within a single ubiquitous processor [30]

Implemented results

VLSI Implementation of above algorithm has composed with two processes: Simulation in Verilog-HDL and Synthesis in VHDL. It has used the 128-word length of the optimum buffer and 0.18-µm standard cell CMOS chip technology. The results have been found that 275 mW power consumption at 200 MHz clock frequency. The evaluation shows that HCgorilla is a high performance and reduced power consumption approach for secure adhoc networks. Figure 5 has proposed the architecture of HCgorilla [30].

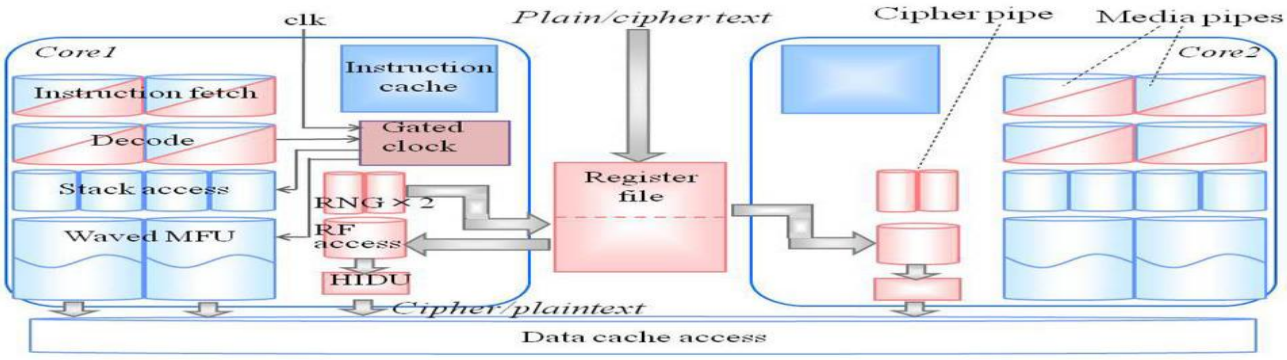

Fig 5: Architecture of HCgorilla [30]

CONCLUSION

In this paper, we have surveyed the FPGA implemented security algorithms for Mobile adhoc networks. We gave a brief description about all the recent schemes discussed above and then implemented results have been provided. In this paper, the great importance of VHDL, Verilog and FPGA has been shown. The Analysis gave a interesting result that the HCgorilla is a high-performance hardware approach for secure multimedia data and Secure Cluster Algorithm provides the rebuilding and recovering mechanism so it is able to resist attacks on the cluster structure. The result shows that FPGA implementation outperforms software and processors implementation. Scopes for further research include some challenges like low power dissipation, reliability, energy saving and testing methodologies.

ACKNOWLEDGMENTS

This work is supported by Department of Electronics, Banasthali University, Rajasthan, India.

REFERENCES

[1] Panagiotis Papadimitratos, Member, IEEE, and Zygmunt J. Haas, Senior Member, IEEE. *Secure Data Communication in. Mobile Ad Hoc Networks*. IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO.2, 2006 pp 343,356.

[2] Mohsen Guizani. "*Security and Trust in Mobile Ad Hoc Networks".* Proceedings of the 4th Annual Communication Networks and Services Research Conference (CNSR'06). 2006.

[3] Konrad Wrona, *"Distributed security: ad hoc networks & beyond"*.Ad Hoc networks security, pompas workshop, 2002.

[4] NIST (National Institute of Security and Technologies). *Wireless Network Security 802.11, Bluetooth and Handheld Devices*. Technical report

[5] Shariful Islam. *Efficient Key Management Scheme for Mobile Ad Hoc Network*. Master of Science. Royal Institute of Technology (KTH) SecLab Department of Computer and System Sciences (DSV). Stockholm, Sweden, 2005.

[6] Adam Burg, Ad hoc networking: concepts, applications, and security. Ad hoc network specific attacks Seminar, Technische Universität München, 2003.

[7] Tor Inge Skaar, Tor-Erik Thorjussen, *Security Specification, Access Control and Dynamic Routing for Ad-Hoc Wireless Networks applied to Medical Emergencies*. Project report Norwegian University of Science and Technology Faculty of Information Technology, Mathematics and Electrical Engineering, 2003.

[8] Tara M., Charles R.Elden,2002. *Wireless security and privacy Best Practices and Design Techniques*, Addison Wesley.

[9] A. T. Abdel-Hamid, S. Tahar, and E. M. Aboulhamid. IP watermarking techniques:survey and comparison. In IEEE International Workshop on System-on-Chip for Real-Time Applications, 2003. ISBN 0-7695-1929-6.

[10] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi. The EM sidechannel(s). In Cryptographic Hardware and Embedded Systems Workshop, volume 2523 of LNCS, pages 29{45, London, UK, August 2002. Springer-Verlag. ISBN 3-540-00409-2.

[11] Algotronix Ltd. AES G3 data sheet Xilinx edition, October 2007. http://www.algotronix store.com/kb_results.asp?ID=7

[12] Shi Zhong, Taghi M. Khoshgoftaar, and Naeem Seliya. Evaluating Clustering Techniques for Unsupervised Network Intrusion Detection. *International Journal of Reliability, Quality, and Safety Engineering*, 2005.

[13] Khaled Labib, V. Rao Vemuri, "Application of Exploratory Multivariate Analysis for Network Security", CRC Press, 2005

[14] Rhodes B., Mahaffey J., Cannady J., "Multiple Self-Organizing Maps for Intrusion Detection" *Proceedings of the NISSC 2000 conference*, Baltimore M.D. 2000.

[15] Shah H., Undercoffer J., Joshi A., “Fuzzy Clustering for Intrusion Detection”. *FUZZ-IEEE*, 2003
[16]http://www.cs.ucdavis.edu/~vemuri/papers/HardwareClustering-Rev7.pdf
[17] F.-X. Standaert, G. Piret, N. Gershenfeld, and J.-J. Quisquater, “SEA: A Scalable Encryption Algorithm for Small Embedded Applications,” in *the Proceedings of CARDIS 2006*, ser. LNCS, vol. 3928, Taragona, Spain, 2006, pp. 222–236.
[18] *Data Encryption Standard*, NIST Federal Information Processing Stan- dard FIPS 46-1, Jan. 1998.
[19] J. Daemen, V. Rijmen, *The Design of Rijndael*. Springer-Verlag, 2001.
[20] F. Macé, F. X. Standaert, J.-J. Quisquater, FPGA Implementation(s) of a Scalabl Encryption Algorithm, IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Volume:16 , Issue: 2 ,Nov. 2007
[21] Kaps J-P. Cryptography for ultra-low power devices. Ph.D. dissertation, Worcester Polytechnic Institute, 2006.
[22] Rivest R, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. In Communications of the ACM, Vol. 21, 1978; 120–126.
[23] O’Rourke CM. Efficient NTRU implementations. Master’s thesis, Worcester Polytechnic Institute, 2002.
[24] Fei Hu et. al., NTRU-based sensor network security: a low-power hardware implementation perspective, Security Comm. Networks. (2008), Published online in Wiley InterScience.
[25] S. Che, J. Li, J.W. Sheaffer,K. Skadron and J. Lach, "Accelerating Compute-Intensive Applications with GPUs and FPGAs," Proc. of IEEE Symposium on Application Specific Processors(SASP). pp.101–107, 2008.
[26] Taeyoon Yoon and Joonseok Park, FPGA Implementation of Network Coding Decoder, IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.12, December 2010
[27] Satyanarayanan, M. Privacy: The Achilles Heel of Pervasive Computing? IEEE Pervasive Computing (2003).
[28] Fukase, M, Uchiumi, H, Ishihara, T, Osumi, Y, & Sato, T. Cipher and Media Possibility of a Ubiquitous Processor: proceedings of International Symposium on Communications and Information Technologies, ISCIT(2009),September 2009, Incheon,Korea., 2009, 343-347.
[29] Sato, T, Imaruoka, S, & Fukase, M. Hardware-Based IPS for Embedded Systems: proceedings of the 13th World Multi-Conference on Systemics, Cybernetics and Informatics,WMSCI 2009, IIII July (2009). Orlando, Florida., 74-79.
[30]Masa-aki FukaseA Double Cipher Scheme for Applications in Ad Hoc Networks and its VLSI ImplementationsTheory and Practice of Cryptography and Network Security Protocols and Technologies, Jaydip Sen, ISBN 978-953-51-1176-4, 2013.

Author’ biography

Dr. Seema Verma obtained her Master and Ph.D degree in Electronics from Banasthali University in 1999 & 2003. She is currently working as Associate Professor of Electronics and Head, Department of Aviation Sciences at Banasthali University. She is Fellow of IETE, Life Member of Indian Science Congress, Life member of International Association of Engineers, (IAENG). She is in the Pearl edition of Who's Who in the World (2013). She is an active research supervisor and 4 Ph.Ds have been awarded under her guidance. She has been frequently invited to present invited or plenary keynote lectures at international conferences in India & abroad. She has presented many papers in various international conferences. She has published many research papers in various journals of repute. She has many projects from UGC (under R7D Major Research project Scheme, UGC Innovative Course Scheme) & AICTE to her credit. She is currently into the editorial board of many international journals in the field Wireless Communication and Coding. Her research areas are Coding theory, TURBO Codes, Wireless sensor networks, Aircraft Ad-hoc networks, Network Security & VLSI Design.

Pooja Srivastava is currently working as Assistant Professor in Department of Electronics at Banasthali University, Rajasthan, India. She received her B.Tech. degree in Electronics and Communication Engineering from Uttar Pradesh Technical University, Lucknow, U.P., India in 2006 and M.Tech. (VLSI Design) from Banasthali University, Rajasthan, India in 2009. She has five year teaching experience and published several research papers in National and International Journals. Her research interest includes Adhoc Networks, Wireless Communication Systems, Turbo Codes, VLSI Design and Fabrication Technology.

Divya Ramawat received her B.Tech. degree in Electronics and Communication Engineering from University of Rajasthan, India in 2009. Currently, she is persuing M.Tech. (VLSI Design) from Banasthali University, Rajasthan, India. Her research interest includes Adhoc Networks, VLSI Design and Wireless Communication Systems.

Nupur Srivastava received her B.Tech. degree in Electronics and Communication Engineering from Uttar Pradesh Technical University, Lucknow, U.P., India in 2012. Currently, she is persuing M.Tech. (VLSI Design) from Banasthali University, Rajasthan, India. Her research interest includes Adhoc Networks, VLSI Design and Wireless Communication Systems.