International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-3 Issue-1, October 2013

Hardware Implementation of Involutional SPN Block Ciphers

Rakhesh Kusagur, Leelavathi G.

Abstract — Consider the two involutional SPN (substitution-permutation network) block ciphers, namely KHAZAD and BSPN, since both of these algorithms adopt SPN structure. Investigation of the energy cost of the FPGA implementation of these two cryptographic algorithms targeted to wireless sensor networks (WSNs) has to be done. Recent trends have seen the emergence of WSNs using sensor nodes based on reprogrammable hardware, such as a field-programmable gate arrays (FPGAs), thereby providing flexible functionality with higher performance and speed than classical microcontroller based sensor nodes. Investigation of the hardware implementation of involutional SPN block ciphers has to be carried out since the characteristics of involution enables performing encryption and decryption using the same circuit. This characteristic is particularly suitable for a wireless sensor node which requires the function of both encryption and decryption. Further, in order to consider the suitability of a block cipher for some of the applications like wireless sensor node, it is most critical to consider the cost of encryption in terms of energy consumption because wireless sensor node is a energy constrained device. Hence, it is appropriate to chose two involutional SPN block ciphers namely KHAZAD and BSPN and analyze their energy efficiency for implementation in the FPGA.

Index Terms— Security, block ciphers, Field programmable gate arrays, involutional.

I. INTRODUCTION

Recent trends in wireless sensor networks (WSNs) include the incorporation of reconfigurable hardware into a sensor node. Typically, the low cost general-purpose microcontroller is supplemented with reconfigurable hardware, such as a field programmable gate (FPGA), to more efficiently execute computationally intensive data processing.

In recent years, several researchers have focused on implementing and analyzing reconfigurable sensor nodes for WSNs. This has included the use of a commercial FPGA functioning as the reconfigurable hardware, such as the atmel series used; while others use specific reconfigurable integrated circuits to achieve the hardware acceleration.
Since an FPGA is not a device especially designed for low power consumption, this becomes an inevitable issue that a FPGA in energy constrained applications like WSN's might introduce more energy cost while providing the higher performance and more flexibility.

Manuscript published on 30 October 2013.
* Correspondence Author (s)
Mr. Rakhesh Kusagur*, VLSI Design and Embedded Systems, VTU Extension Center,UTL Technologies Ltd., Bangalore, India.
Mrs. Leelavathi G, VLSI Design and Embedded systems, VTU Extension Center, UTL Technologies Ltd., Bangalore, India.

II. THE HARDWARE SYSTEM

A. Involutional block ciphers

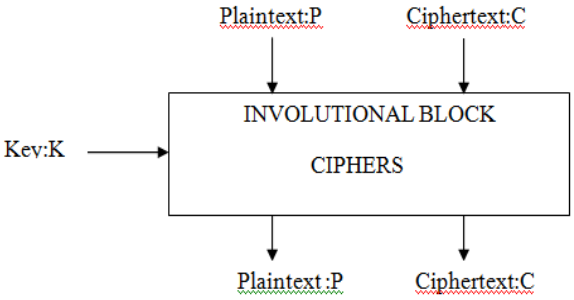

Fig 1: Involutional block ciphers

The investigation of FPGA implementation and energy cost analysis of two light weight involutional block ciphers, such as KHAZAD and BSPN for WSNs application depend on speed and higher flexibility. The FPGA implementation based on two design factors: The structure of design and the resource utilization of FPGA. By implementing cipher KHAZAD and BSPN in different methods, we further analyze the dynamic power of circuit and calculate the energy cost of the design and compare the implementation of two scenarios: full cipher implemented by hardware and cipher implemented by hardware as well as software.

B. Structure of KHAZAD

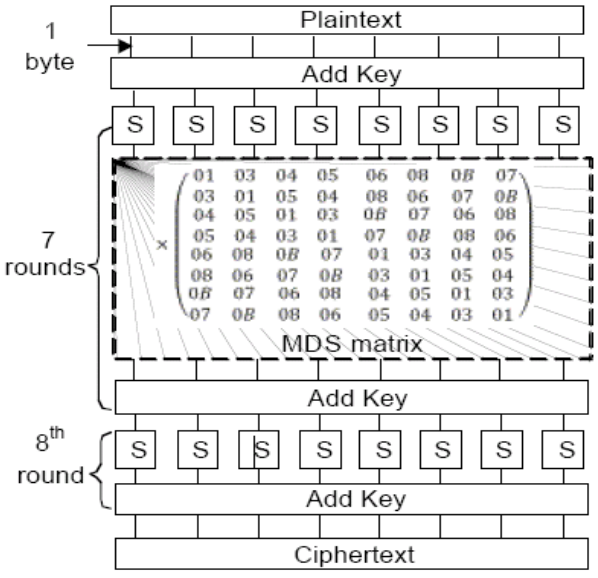

Fig 2: Structure of KHAZAD algorithm

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Figure 2 shows the complete structure of the KHAZAD algorithm. 64-bit plaintext,128 bit key are the inputs,64 bit ciphertext is the output. Plaintext is XOR'd with the addkey. The 64-bit output of addition is divided as eight 8bit groups. Each 8bit the input to the each 8 bit S-box's. MDS(maximum distance separable)matrix is used for the linear transformation. There is no need of linear transformation for the last round. Finally the ciphertext is produced. Inverse operations have to be carried out for the decryption process.

C. Structure of BSPN

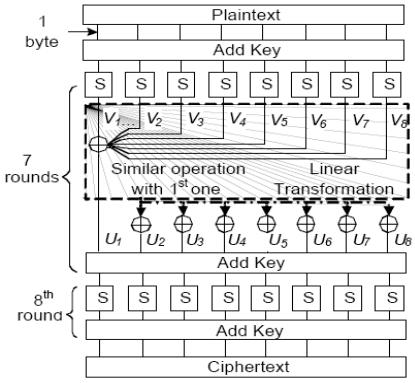

Fig 3:Structure of BSPN algorithm

Figure 3 shows the complete structure of the BSPN algorithm. 64-bit plaintext,128 bit key are the inputs,64 bit ciphertext is the output. Plaintext is XOR'd with the addkey.

The 64-bit output of addition is divided as eight 8bit groups. Each 8bit the input to the each 8 bit S-box's. Linear transformation is simple XOR operation. There is no need of linear transformation for the last round. Finally the ciphertext is produced. Inverse operations have to be carried out for the decryption process.

III. DESIGN AND IMPLEMENTATION

A. Substitution-Permutation Networks

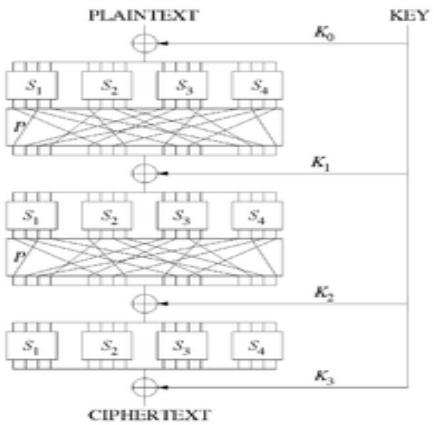

Fig.4:Substitution-permutation network with 3 rounds

A sketch of a Substitution-Permutation Network with 3 rounds,which encrypts the 16 bit plaintext into a ciphertext block of 16 bits. The S-boxes are the S_i's, the P-boxes are the same P, and the round keys are the K_i's.

One important type of iterated block cipher known as a *substitution-permutation network (SPN)* takes a block of the plaintext and the key as inputs, with several alternating rounds consisting of a substitution stage followed by a permutation stage—to produce each block of ciphertext output. The non-linear substitution stage mixes the key bits with those of the plaintext. The linear permutation stage then dissipates redundancies.

A *substitution box (S-box)* substitutes a small block of input bits with another block of output bits. This substitution has to ensure the invertible property (hence decryption). An S-box will be secure if it has the property that changing one input bit will change about half of the output bits on average, exhibiting the property what is known as the avalanche effect-i.e. any changes made to the input bits will directly affect the output bits..

A *permutation box (P-box)* is a permutation of all the bits: it takes the outputs of all the S-boxes of one round, permutes the bits, and gives them into the S-boxes of the next round. A good P-box will be having the property that the output bits of any S-box are distributed to as many S-box inputs as possible.

At each round, the round key (obtained from the key with some simple operations, for instance, using S-boxes and P-boxes) is combined using some group operation, typically XOR.

Decryption is done by just reversing the process (using the inverses of the S-boxes and P-boxes and applying the round keys in reversed order).

B. KHAZAD Algorithm

KHAZAD is named after Khazad-dum, the "Mansion of the Khazad," which in the tongue of the Dwarves is the name of the great realm and city of Dwarrowdelf. KHAZAD is a legacy-level block cipher designed by Vincent Rijmen and Paulo S.L.M Barreto. As such, it operates on data blocks of 64- bits length, and uses 128 bits key length. It has been submitted as a candidate algorithm for the cryptographic primitive evaluation effort, and at the same time its tweaked form was selected as finalist. KHAZAD is an iterated 64-bit block cipher with 128-bit keys. It contains 8 rounds; each round consists of eight 8-bit to 8-bit S-box parallel lookups, a linear transformation (multiplication by a constant MDS diffusion matrix) and round key addition. The S-box and the diffusion matrix were chosen in a way which guarantees that encryption and decryption are the same operation except in the round subkeys. KHAZAD belongs to the same family of block ciphers as the AES algorithm, RIJNDAEL, which is very similar to the SHARK cipher.

C. BSPN Algorithm

Byte-wise SPN (BSPN) is a compact block cipher we suggest to use in WSNs, which provides moderate security to the energy limited environment. It has no apparent weaknesses and is resistant to both the differential and linear cryptanalysis attacks. In the next section, we will show that it provides good energy performance applied in WSNs compared to other candidate block ciphers. BSPN is a block cipher with an 64bit block size and 64-bit (or larger) key size. It has 8 rounds of operation and each round of operation includes add round key, substitution and linear transformation as shown in Fig. 4.3. It uses an 8×8 S-box, which functions as a nonlinear transformation between 8 bits of input and 8 bits of output. The result of the linear transformation, *U*, which is achieved by bitwise XORing the output bytes, *Vi*, of the other seven S-boxes after adding the round key.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

In the figure, the connection between each component represents one byte of data and S represents an 8×8 S-box. The "Add Key" operation is achieved through bitwise XOR of the 64-bit data and the 64-bit round key.

IV.SOFTWARE IMPLEMENTATION

A. Xilinx

Xilinx ISE (Integrated Software Environment) is a software tool produced by Xilinx for synthesis and analysis of HDL designs, enabling the developer to synthesize ("compile") their designs, examine RTL diagrams, perform timing analysis, simulating a design's reaction to different stimulus and configure the target board with the programmer. In the present work Xilinx 13.2 ISE is being used for coding and development along with ADEPT from digilent for hardware linking.

B. Verilog-Coding Language

Verilog HDL is one of the two most common Hardware Description Languages (HDL) used by integrated circuit (IC) designers. The alternative one is VHDL. HDL allows the design to be simulated earlier in the design cycle in order to correct errors or experiment with different architectures. Designs described using HDL are technology-independent, they are easy to design and debug, and are usually more readable than schematics, specifically for large circuits.

Verilog can be used to describe the designs at four levels of abstraction:

1. Algorithmic level (much like c code with if, case and the loop statements).
2. Register transfer level (RTL uses registers connected by Boolean equations).
3. Gate level (interconnected AND gates , NOR gates etc.).
4. Switch level (the switches are MOS transistors inside gates).

The verilog language also defines constructs that can be used to control the input and output of simulation

V.TESTING AND RESULTS

The simulation of the KHAZAD and BSPN algorithms has been carried out in the Xilinx Isim simulator. The simulation waveforms are shown in the figures 5 and 6 for the KHAZAD and BSPN algorithms respectively.

There are totally 7 rounds in the both KHAZAD and BSPN algorithms. To increase the security of the algorithms extra round has been added, for which the new algorithm has been proposed.

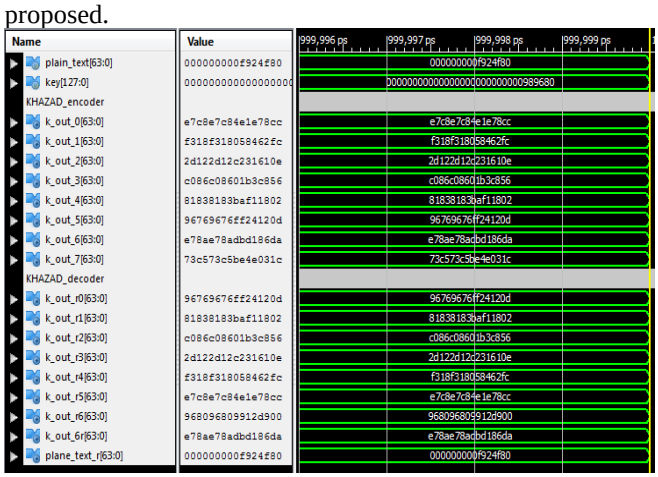

Fig 5:Simulation results of KHAZAD algorithm

The figure 5 depicts the simulation of the KHAZAD algorithm with 8 rounds which includes both encryption as well as decryption.

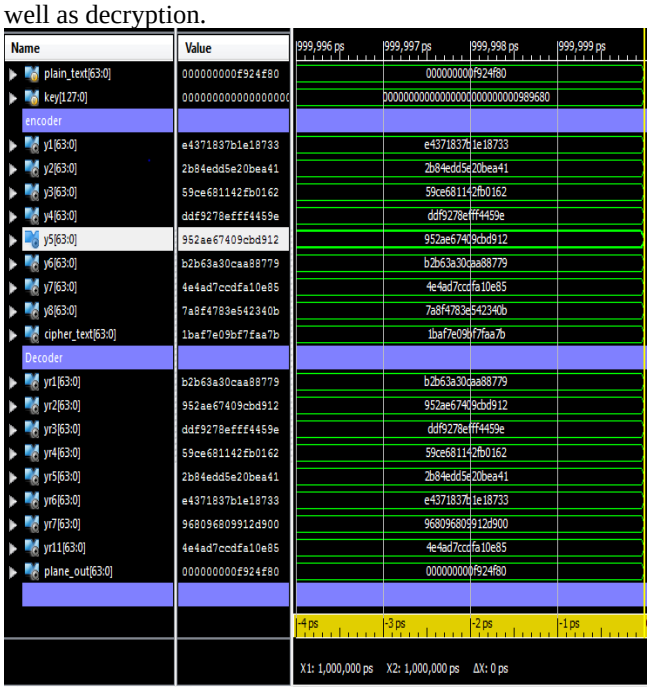

Fig.6: Simulation results of BSPN algorithm

Figure 6 depicts the simulation of the BSPN algorithm which includes both encryption as well as decryption. The algorithm consists of 8 rounds. Simulation has been carried out in the Xilinx ISE simulator.

VI. CONCLUSION

It has been focused on hardware implementation of involutional block ciphers in reconfigurable WSN nodes. Results show that:

1. In contrast to KHAZAD algorithm there is a simple linear transformation in the BSPN algorithm because of which area consumed by the BSPN will be lesser.
2. One extra round has been added to both algorithms because of which security of the algorithms have been obviously increased to some extent.
3. From power analysis results it can be seen that BSPN algorithm is consuming less power as compared to KHAZAD algorithm.

ACKNOWLEDGMENT

I would like to take this opportunity to express my deep sense of gratitude to **Dr. V.Venkateswarlu**, HOD and Principal, VTU Extension Centre, UTL Technologies Limited, Bangalore, for his invaluable inspiration and guidance without which the project work would not have progressed to its present state. I cannot forget the constant encouragement and help provided by my internal guide, **Mr. Leelavathi**, Visiting Professor, VTU Extension Centre, UTL Technologies Limited, Bangalore, who considered me like a friend and made me feel at ease in times of difficulty during my project work. I express my sincere thanks to him. I do not know how to express my thanks to my external guide **Mr. V. Ganesh Kumar**, Project manager, Ultraa Chipp Tecchnologies,

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Bangalore, who provided constant encouragement whenever I faced difficulties in my project work. I really express my sincere thanks to him. I would finally like to extend my gratitude to all the teaching and non teaching staff both at VTU Extension Centre, UTL Technologies Limited, Bangalore.

REFERENCES

[1]. Xueying Zhang, H.M. Heys, and Cheng Li, "*FPGA Implementation of Two Involutional BlockCiphers Targeted to Wireless Sensor Networks",* 6th International ICST Conference on Communications and Networking in China, 2011.

[2]. P. Muralidhar and C.B.Rama Rao, "Reconfigurable Wireless Sensor Network Node based on NIOS core," In Proc. of *4th Wireless Communication and Sensor Networks (WCSN 2008)*, pp. 67-72, Jhalwa, India, Dec. 2008.

[3]. E. Susu, M. Magno, A. Acquaviva, and D. Atienza, "Reconfiguration Strategies for Environmentally Powered Devices: Theoretical Analysis and Experimental Validation", *Transactions on High-Performance Embedded Architectures and Compilers I (HiPEAC I)*, pp. 341-360, 2007.

[4]. J. Portilla, A. de Castro, E. de la Torre, T. Riesgo, "A Modular Architecture for Nodes in Wireless Sensor Networks", *Journal of Universal Computer Science(JUCS)*, vol. 12, no 3, Mar. 2006, pp. 328-339.

[5]. X. Zhang, *Energy Efficiency in Secure Wireless Networks*, M.Eng Thesis, Memorial University of Newfoundland, 2010.

[6]. Y. Wang, G. Attebury, B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," IEEE Communications Surveys & Tutorials, vol.8, no.2, pp. 2-23, 2006.

[7]. W. K. Koo, H. Lee, Y. H. Kim and D. H. Lee, "Implementation and Analysis of New Lightweight Cryptographic Algorithm Suitable for Wireless Sensor Networks," in *Proc of 2008 Information Security and Assurance (ISA 2008)*, pp.73-76, Korea, April 2008.

[8]. A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, "Energy Analysis of Public-key Cryptography for Wireless Sensor Networks," *in Proc of 2005 Pervasive Computing and Communications (PerCom2005)*, pp.324-328, Germany, March 2005.

[9]. R. Tahir, M. Y. Javed, M. Tahir and F. Imam, "LRSA: Lightweight Rabbit Based Security Architecture for Wireless Sensor Networks,"*in Procof 2008 Intelligent Information Technology Application (IITA'08)* ,vol.3, pp.679-683, China, Dec. 2008.

[10]. M. Henricksen, "Tiny Dragon - An Encryption Algorithm for Wireless Sensor Networks," *in Proc of 10th High Performance Computing and Communications, (HPCC '08)*, p.p. 795-800, 25-27 Sept. 2008.

[11]. A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, "SPINS: Security Protocols for Sensor Networks," *ACM Wireless Networks*, vol.8, no. 5, pp. 521-534,Sept. 2002.

[12]. A.J. Menezes, P. van Oorschot, and S.A. Vanstone, *Handbook of Applied Cryptography*.CRC Press, 1997.

[13]. J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister, "System Architecture Directions for Networked Sensors," *in Proc. Of ACM ASPLOS IX*,pp. 93-104, Nov 2000.

[14]. X. Zhang, H.M. Heys, and C. Li, "An Analysis of Link Layer Encryption Schemes in Wireless Sensor Networks," *in Proc of IEEE International Conference on Communications (ICC 2010), Cape Town, May 2010.*

[15]. B. Schneier, *Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C*. John Wiley & Sons, 1996.

Mr. Rakhesh Kusagur is pursuing his final year M.Tech degree in VLSI Design and Embedded Systems at VTU Extension Center, UTL Technologies Ltd., Bangalore. His research interest includes SOC verification and embedded systems.

Mrs. Leelavathi G. is working as a visiting professor in Dept. of VLSI Design and Embedded Systems at VTU Extension Center, UTL Technologies Ltd., Bangalore. His research interest includes embedded systems.