International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359

Research Article | **February 2013**

FPGA Implementation for Energy Efficiency in Secure Wireless Sensor Node–A Critical Review

C. Karthik Sendhil Kumar
Department of ECE,
Sethu Institute of Technology,

R.Sukumar
Department of CSE,
Sethu Institute of Technology,

M.Nageswari
Final year ECE student,
Sethu Institute of Technology,

Abstract:

In this paper, we propose the hardware implementation of involutional block ciphers with low energy cost for cryptographic algorithm to WSNs by FPGA implementation. Formerly, microcontroller based sensor nodes are designed like PIC microcontroller, AT Mega128 microcontroller, MSP430.But it have some drawbacks .1) High processing time2) It consumes large amount of energy3) It have less security4) Possible to missing some events5) More time delay6) It affects execution of other programs. This paper insists to use the Field Programmable Gate Array to overcome those problems and enable providing higher performance and more flexibility than microcontroller based sensor nodes. The characteristics of involutional block perform both encryption and decryption by using same circuit.Further,we analyse their energy efficiency in FPGA implementation by choosing two involutional block ciphers KHAZAD and BSPN which considering different design factors such as structure of design and the resource utilization of FPGA.

Keywords: ***Energy efficiency, Security, Wireless Sensor Networks, FPGA, Involutional Blocks.***

I. INTRODUCTION

At present, the incorporation of reconfigurable hardware into a sensor node is include with wireless sensor networks.Typically,the low cost general-purpose microcontroller is supplemented with reconfigurable hardware, such as FPGA to more efficiently execute computationally intensive data processing.Now,several researchers have focused on implementing and analysing reconfigurable sensor nodes for WSNs.Some research utilizes a commercial FPGA functioning as reconfigurable hardware. Xilinx Spartan 3 FPGA[12] is used to design the reconfigurability by modular architecture.FPGA from Actel IGLOO series[13] which consumes as low as 2 microwatt of power.Because of battery-powered and resources constrained device, light weight block cipher is mostly used for security in WSNs.Main feature of involutional block is same piece of logic circuit can be shared for both encryption and decryption operations. In this paper, investigating FPGA implementation and energy cost analysis of two light weight involutional block ciphers, such as KHAZAD[14] and BSPN[15,16] 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

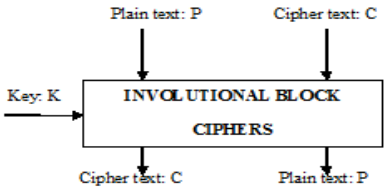

Fig. 1 Involutional block cipher

cipher KHAZAD and BSPN in different methods, we further analyse 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.

II. RELATED WORK

A. Involutional block ciphers

F (F(x)) =X

An involutional block cipher means block cipher with an involutional characteristics. An involutional block cipher encrypts the plaintext to generate the cipher text and exact same algorithm is used for decrypts the cipher text to generate the plaintext. As sensor node is a resource-limited device, involutional block ciphers provide to achieve security goals in WSNs.

B. Common features of an involutional SPN block cipher

Both KHAZAD & BSPN adopt the 'Substitution Permutation Network 'structure which have three basic components: substitution, permutation &addition of round keys. Both involutional blocks have 8 rounds of operation and make 8*8 S-box and 64bits block size. In encryption," Add round key operation is performed before "Linear transformation"operation.It is the reverse order in decryption[round key addition is bit wise XOR].No Linear transformation is involved in last round operation and extra round key addition at cipher start. The nine round keys involved in key addition operations are generated based on cipher key is known as "Round key Expansion or key Scheduling".

C. ***Comparison of components of KHAZAD & BSPN***

The structures of two ciphers are compared based on substitution, linear transformation and add round keys.

1. ***Substitution:***The involutional S-box of KHAZAD was designed by Pseudo-random S-box generation. An appropriate S-box is chosen among these random S-boxes, which satisfies involutional functionality and other security requirements. But this method may not be efficient for hardware implementation under some conditions. For this purpose, the designers further proposed an alternative S-box, which is based on the structure of connecting small involutional S-boxes with an involutional permutation.There is no specific S-box provided for BSPN which is designed based on AES S-box and uses multiplicative inverse in GF (2^8) and affine transformation [17]. Although there are two fixed points (0*00 and 0*FE), there is no evidence that fixed points can lead to attack on the cipher.
2. ***Linear Transformation:***In KHAZAD linear transformation is based on MDS code which is selected with criterion that achieves efficient implementation for both software and hardware. But final decision is made by two factors like lowest possible hamming weight and integer values.In BSPN, linear transformation is byte oriented which produces a byte following the output of S-box by XORing the output of other S-boxes.
3. ***Key Addition and Key Expansion:*** Both KHAZAD and BSPN apply key by bitwise XOR,The round keys are generated from cipher key by key expansion processes to described in [14] and [18].Compared to KHAZAD,BSPN has more complicated key expansion algorithm. In WSNs, cipher key will be changed infrequently, which means key expansion algorithm need be executed infrequently. Since generated round keys can be stored, thereby minimizing impact to low energy consumption of the node.

III. HARDWARE IMPLEMENTATIONS

The hardware is implemented by Verilog HDL code with FPGA. In our design, the key expansion is only processed during initial setup period or when a new cipher key is established.

A. Interfaces and Timing Requirements

In our design, both cipher KHAZAD and BSPN use same interfaces and timing requirements. So that, it is convenient to understand and compare these two designs.

B. ***Substitution***

The implementation of an 8*8 box can be achieved in two ways.1) Using Look Up Table (LUT) to implement Boolean function which is constructed by combinational logic(for low time delay) 2) Using the configurable Block RAM(BRAM) core which is embedded in FPGA device(for fully utilize the resources). Both KHAZAD and BSPN have 64bit block size, the whole substitution layer can also be designed for different purposes like using only one S-box circuit for minimizing area and using 8 S-box circuits in parallel for increasing speed.

1. ***LUT vs. BRAM:*** The LUT will generate eight 8 Boolean functions to represent the S-box outputs by FPGA synthesis tool. BRAM needs to be configured and generated before using, and the memory size should not exceed the maximum size of FPGA.In LUT design, the output will be valid after the input is given, while in BRAM design, the output will not be valid until next clock rising edge because of synchronous structure. Furthermore, the LUT has less time delay than that of BRAM.
2. ***Small Area vs. High Speed:*** For the purpose of small area, only one S-box circuit is used in the design which serially generates the output value byte by byte. It needs eight clock cycles to finish 64bit of substitution. We use 3bit counter and demux to route the appropriate register to store S-box output value.For the purpose of high speed, eight S-box circuits are used in the design, which simultaneously generate the full 64bit output in one clock cycle.Both area and speed factors will affect the sensor node. Processing the data for long time or using large number of transistors will both lead large energy cost.

C. Linear Transformation

1. ***Cipher KHAZAD:*** We implement the KHAZAD linear transformation by using combinational logic to make the circuit work more efficiently and to avoid using a complicated multiplier circuit for the matrix.
2. ***Cipher BSPN:*** Compared to KHAZAD, BSPN has simple linear transformation.

D. ***SPN core circuit sharing***

To achieve better power efficiency, the key expansion process and data encryption/decryption processes are regarded as two processes. To satisfy those achievements, we use SPN core designed. A counter is used for round number and its maximum value is decided by the specific cipher. Multiplexers are used to apply data for process.

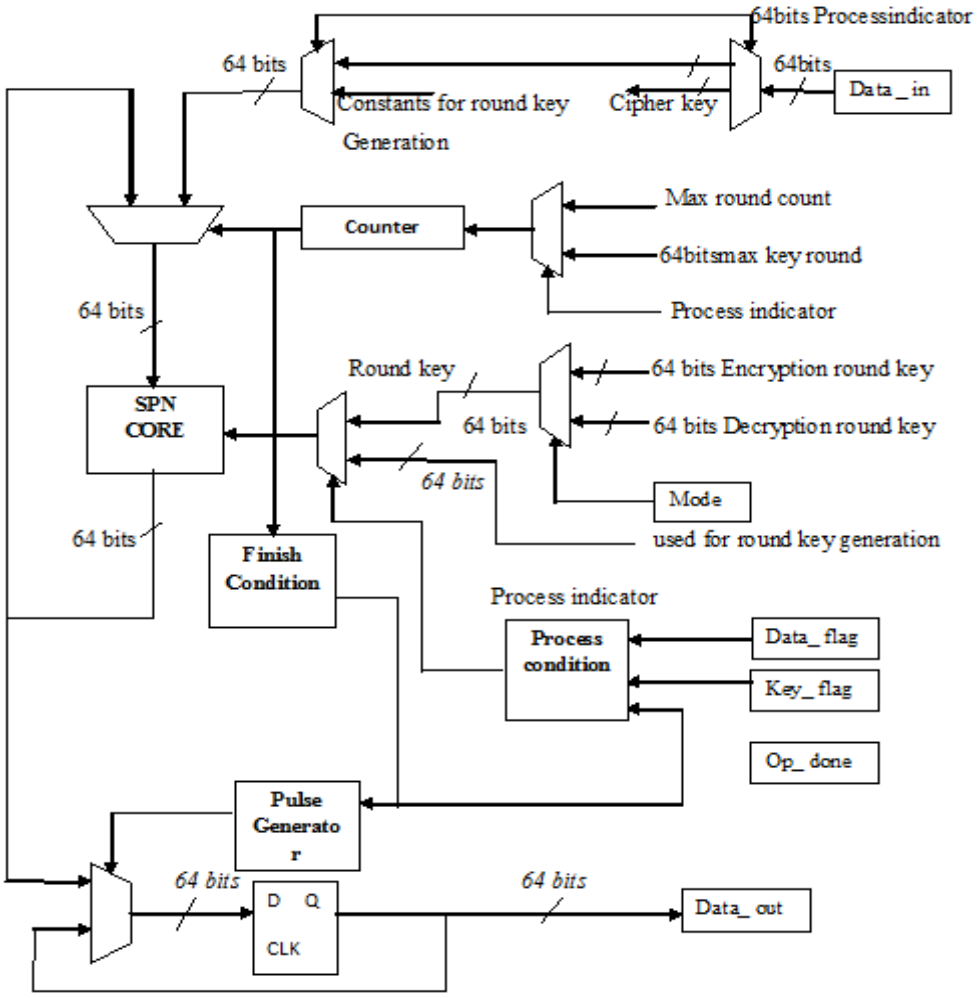

Fig. 2 Structure of SPN

IV. RESOURCE UTILIZATION

We have chosen Xilinx Spartan 3 series device Xc3s200 [19] which is low end, low power FPGA. We use EDA tool Modelsim for simulation and Xilinx ISE for synthesis. Both cipher KHAZAD and BSPN are implemented using four different methods, that is, 1) one S-box LUT circuit2)8 S-box LUT circuit 3)one S-box BRAM circuit4)8 S-box BRAM circuit. We can compare the energy performance between cipher KHAZAD and BSPN at different levels, that is 1) full hardware including key scheduling and data operation2) only data operation3) different structures of linear transformation.

A. LUT method vs. BRAM method

We first investigate the effects of different methods applied to a design. Here, we use labels BSPN-64 and BSPN-128 to represent the cipher BSPN key size 64bits and 128bits, respectively. The S-box constructed by LUT or BRAM is a dominant factor for the total equivalent gate count for design. This is because the equivalent gate for count of BRAM is greatly larger than the same function using LUT. Compared to using LUT, the number of occupied slices is smaller with use of BRAM. Furthermore, designs using eight S-box circuits introduce more FPGA resources than using only one S-box and it will increase the speed in encryption and decryption process.

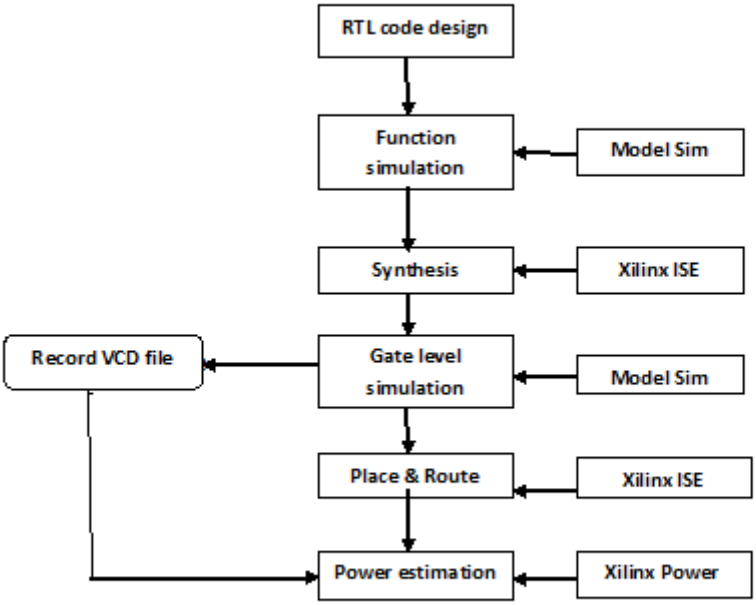

Fig. 3 Power estimation flow by Xpower

B. *Full Cipher implementation*

In this subsection, we focus on comparing the hardware implementation of cipher KHAZAD and BSPN-128 with both of them using 128-bit key..

C. *Data Operation implementation*

For WSNs applications, the key scheduling operation is processed infrequently. Our design's purpose is to apply the circuit to a reconfigurable WSNs, the cooperation of hardware and software can be used: first, the MCU can generate the round keys by software and store them in its memory for future use; then MCU indicates the hardware to directly load the round keys and release the memory for other use. Nine 64bit registers are used to store encryption round keys for future use. The total equivalent gate count for cipher KHAZAD is much larger than that of BSPN. At the same time, total equivalent gate count for using 8 S-boxes are larger than that of using one S-box circuit.

D. Implementation for linear transformation

The linear transformation part of these two ciphers is the major difference because of other basic components of SPN is almost same: 1) BRAM makes the S-box using same resources of FPGA2) the operation of add round keys use the same amount of XOR logic. The amount of XOR logic used by cipher KHAZAD is larger than that of BSPN, which leads to difference of resource consumption between these two ciphers.

V. ENERGY CONSUMPTION ANALYSIS

FPGA power includes two parts: static power and dynamic power. Static power is the intrinsic power of the device and cannot be changed. It exits once the chip is powered ON, even if there is no activity in the device. It includes transistor leakage, power consumed internally and power dissipated in external termination resistors. Dynamic power is caused by switching activity of CMOS transistors. Dynamic power is only consumed when the state of transistors changes, which depends on specific implementation of the design. A design can consume less power if it is implemented in an appropriate way.

Xilinx Xpower is a tool providing the power estimation for a FPGA design based on switching activity of transistors which can be analysed after the process of "place & route"(capacitance model used for power calculation).Methods for power estimation using Xpower:1)rough estimation by setting an expected toggle rate2)more accurate estimation by providing detailed transistor switching activity. Here, we choose second method for accuracy. The switching activity of circuit can be recorded in VCD file at different time slots which can be obtained by simulation when we simulate the gate level net list of the design. Another purpose of gate level simulation is to examine whether Register Transfer Level (RTL) code is synthesized into gate level net list. Finally, Xpower reads VCD file and generates the power estimation report which is depend on accuracy of switching data.

A. Energy cost analysis for hardware implementation

We simulate the gate level net list of designs and calculate the energy consumed by processing encryption or decryption of a block size (64bits) of data which do not include key scheduling process. We focus an energy efficiency of cipher KHAZAD and BSPN.

1. ***LUT vs. BRAM:*** The power of design using 8 S-boxes is larger than that of using one S-box but the relation of energy cost is the reverse because operation time for one block size of data using 8 S-boxes is much faster than that of using one S-box.The design using BRAM consumes less energy than the design using LUT. Because BRAM is designed and optimized directly for memory function, while LUT is designed for general-purpose usage.
2. ***KHAZAD vs. BSPN:*** We simulate cipher KHAZAD and BSPN-128; the power estimation is based on structure of BRAM since it is the most energy efficient method. In this part, we investigate two scenarios:
   1. Results of Full Cipher Hardware Implementation

   Cipher KHAZAD consumes much more energy cost than BSPN, for the same cipher, the 8 S-box BRAM structure is more energy efficient. BSPN with eight BRAM S-boxes can achieve the least energy consumption among these four implementations.
   2. Results of Hardware and Software Cooperation

   It includes two major parts:1) The energy cost of key scheduling by software 2) the energy cost of data encryption/decryption by hardware . Although the energy consumption of software implementation is more than hardware implementation, it does not mean an FPGA should be incorporated into a sensor node, which is not originally designed as a reconfigurable sensor node. The reason is that an FPGA is not a power saving device, as it consumes much more static energy than CPU ASIC.

VI. CONCLUTION

For both cipher KHAZAD and BSPN, the implementation using eight S-boxes achieves better energy performance than using one S-box. As the number of bytes of data increases, the cooperative method achieves better energy cost. A cooperative approach is preferred over a pure hardware implementation and greatly preferred over a pure software implementation. By implementing cipher KHAZAD and BSPN with different methods, We can find the following results as such 1) Cipher BSPN achieves better energy performance than cipher KHAZAD due to simplicity of linear transformation and 2) Ciphers using BRAM to implement 8 parallel S-boxes can achieve better energy performance.

REFERENCES

1. Zhang X, Heys HM, and Li C (2011) "FPGA Implementation of Two Involutional Block Ciphers targeted to wireless sensor networks (invited)," in Proc. Of *the 2011 international conference on communications and Networking in China(Chinacom'11),* Harbin, China
2. Abidalrahman Moh'd, Nauman Aslam, William Phillips, William Robertson, Hosein Marzi (2012)"SN-SEC: A Secure Wireless Sensor plat-form with hardware cryptographic Primitives ,"in proc. of *Pers ubiquit comput,DOI 10.1007/s 00779-012-05663-9*
3. Yamada A, Schneider W (2009) survey on the current status of research and development (R&D) of cryptographic technology in the European Commission
4. FIPS PUB-197 (2001) Advanced encryption standard (AES). National Institute of Standards and Technology, U.S. Department of Commerce. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
5. Majeed J (2005) "FPGA based communication security for wireless sensor networks," in Proc. Of the 4th international conference *on Electronic. Signal Processing and Control (WSEAS'05),* Rio de Janeiro, Brazil
6. Muralidhar P, and Rama Rao C (2008)"Reconfigurable wireless sensor network node based on NIOS core," in Proc. *4th Wireless Communication and Sensor Networks (WCSN'08),* pp 67-72
7. Peter S, Steclina O, Portilla J, Torre E, LandendoerferP,andRiesgo T (2009)"Reconfiguring crypto hardware accelarators on Wireless sensor nodes," in Proc. Of *the 6th sensor ,Mesh and Ad hoc Communications and Networks Workshops,(SECON'09 workshops),*Rome, Italy
8. Krasteva YE, Portilla J, Carnicer JM, Torre E, Riesgo T(2008)"Remote HW-SW reconfigurable wireless sensor nodes," in Proc. Of *the 34th Annual Industrial Electronics (IECON'08),* pp 2483-2488, Orlando, FL
9. Mihel J, Magjarevic R (2009)"FPGA based two-channel ECG sensor node for wearable applications," in Proc. Of *the 4th European Conference of the International Federation for Medical and Biological Engineering (IFMBE).* Springer Berlin Heidelberg22:1208-1211
10. Hinkelmann H, Zipf P, and GlesnerM(2006)"Design concepts for a dynamically reconfigurable wireless sensor nodes," in Proc. Of *the 1st NASA/ESA Conference on Adaptive Hardware and Systems (AHS'06),* pp 436-441
11. Susu E, Magno M, Aquaviva A, and Atienza D(2007)"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
12. Portilla J, de Castro A, de la Torre E, Riesgo T (2006) A Modular architectures for nodes in wireless sensor networks. *Journal of Universal Computer Science (JUCS)*12(3):328-339
13. Belhedj H, Aggraval V, Pradhan A, and Zerrouki A. "Power Aware FPGA Design,"[online].Available at: http://www.actel.com/documents/Power_Aware_WP.pdf
14. Barreto PSLM, and Rijmen V "The KHAZAD legacy –level Block cipher," [online]. Available at: http://www.larc.usp.br/~pbarreto/KHAZADpage. Html

15. Youssef A, Tavares SE, and Heys HM (1996)"A new class of supstitution-permutation networks," in Proc. Of *workshops on Selected Areas in Cryptography (SAC'96), Queen's University,* Kingston, Ontario
16. Zhang X, Heys HM , and Li C (2010)"Energy Efficiency of symmetric key cryptographic algorithms in wireless sensor networks," in Proc. Of *25th Biennial Symposium on Communications (QBSE'10)*, Kingston, Ontario
17. Daemen J, Rijmen V (2002) The design of Rijndael : AES- The Advanced encryption Standard. Springer, New York
18. Zhang X (2010) Energy Efficiency in secure wireless sensor networks. M. Eng, Thesis, Memorial University of Newfoundland
19. Xilinx web site: www.xilinx.com