Journal of Electrical Engineering and Electronic Technology

Short Communication

A SCITECHNOL JOURNAL

High-Performance Block Cipher Using Flexible Architecture

A Sindhu*

Department of Electronics Engineering, Bangalore University, Karnataka, India

***Corresponding author:** A Sindhu, Department of Electronics Engineering, Bangalore University, Karnataka, India, Tel: 9786258150; E-mail: Appusanthi1997@gmail.com

Received date: 22 February, 2023, Manuscript No. JEEET-23-89877;

Editor assigned date: 24 February, 2023, PreQC No. JEEET-23-89877 (PQ);

Reviewed date: 10 March, 2023, QC No JEEET-23-89877;

Revised date: 21 April, 2023, Manuscript No. JEEET-23-89877 (R);

Published date: 28 April, 2023, DOI: 10.4172/2325-9833.1000955

Abstract

Lightweight cryptography has been an important area of cryptographic research in recent years. In this project, a high throughput and flexible hardware implementations of the SPECK light weight block cipher is presented. In the SPECK block cipher, to reduce critical path delay, a tree structure for implementation of Sklansky adder which is an efficient parallel prefix adder operation is used. Simon cipher supports the variable key sizes (128, 144,192, and 256) bits and block sizes (64, 96, and 128) bits is also implemented by using the parallel prefix adder structure reduce the critical path delay.

Keywords: Cryptographic; Simon; Speck; Delay; Block cipher

Introduction

Lightweight cryptography has been an important area of cryptographic research in recent years. Different lightweight block ciphers with various design strategies have been presented. The Advanced Encryption Standard (AES) is one of the most important and applicable block ciphers in hardware and software for low resource devices, the AES is a too expensive block cipher. Therefore, many lightweight block ciphers have been proposed to reduce the costs of hardware consumption than that of AES. Lightweight block cipher algorithms play an important role in the security for resource constrained devices, such as Radio Frequency Identification (RFID) tags, smart cards, and Wireless Sensor Network (WSN) nodes. Simon are lightweight block cipher families with 32 bits to 128 bits block size and 64 bits to 256 bits key length, which is suitable for lightweight hardware implementation such as embedded CPUs that are used in the low area cryptographic application systems [1]. The first method is based on high level synthesis to give more flexibility and to achieve suitable throughput. The second method is based on a bit serialized structure to achieve the minimum area and cost in the design. In this method, the structure only used 34 slices on spartan-3 FPGA. This implementation of Simon consumed 36 slices on a spartan-3 FPGA and 13 slices on a spartan-6 FPGA. The focus of this paper is the design and implementation of efficient VLSI structures for the Simon block ciphers. The throughput, execution time, and flexibility of these block ciphers are important factors for hardware implementations [2]. Therefore, the proposed structures are implemented based on efficient components for high throughput and versatile applications.

Description

In this subsection, we describe the proposed architectures for implementing the Speck block cipher. In this cipher the modular adder (mod 2n) is the main block which has the direct impact on Critical Path Delay (CPD) and hardware consumption. In the following, the structure of the modular adder based on a parallel prefix adder is presented [3]. The proposed structure of the Speck blocks cipher. In this design, during the first clock cycle, the start signal is set to “1” and the 2n-bit plaintext P(2n-1: 0) is applied to the structure and stored in two registers Reg 1 and stored in two registers Reg 1 and Reg 2. Then, in the second clock cycle, the start signal is set to “0” for computing the following rounds (Figure 1).

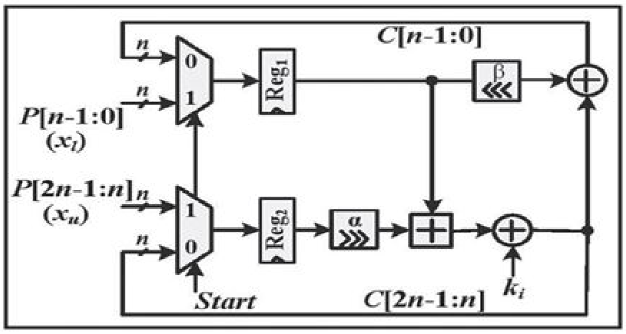


Figure 1: The second clock cycle.

The intermediate results are stored in the same registers. Computations in each round consist of two shift operations, two bit wise XOR operations and one modular adder mod 2n. In the last step, the value of the final round key kr-1 is added to the output of the modular adder for generating the 2n-bit cipher text [4]. The key scheduling process in the Speck cipher for three cases m=2, 3, and 4 is shown in Figure, respectively. The master key is divided into key words k0 to km-1. In the first clock cycle, the Start signal is set to “1” and the words k0 to km-1 are loaded into the registers Reg 1 to Reg 4, respectively. During the second clock cycle, the start signal is set to “0.” In this mode, Reg 1 to Reg 3 are configured as shift registers and other key words k4 to kr-1are generated [5].

The intermediate results are stored in the same registers. Computations in each round consist of two shift operations, two bit-wise XOR operations and one modular adder mod 2n. In the last step, the value of the final round key kr-1 is added to the output of the modular adder for generating the 2n-bit cipher text. The key scheduling process in the Speck cipher for three cases m=2, 3, and 4, respectively. The master key is divided into key words k0 to km-1. In the first clock cycle, the start signal is set to “1” and the words k0 to km-1 are loaded into the registers Reg 1 to Reg 4, respectively. During the second clock cycle, the start signal is set to “0.” In this mode, Reg 1 to Reg 3 are configured as shift registers and other key words k4 to kr-1 are generated [6].

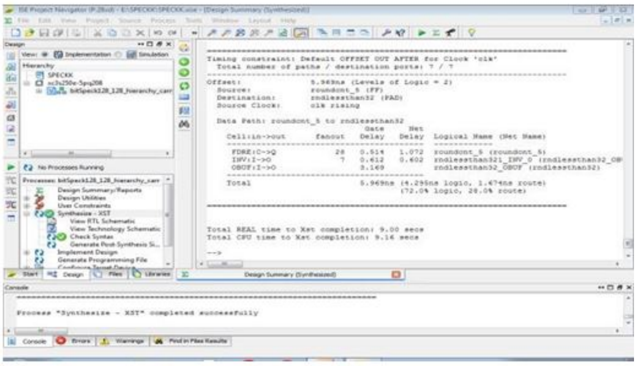
The critical path delay in these structures is reduced compared with the CRA. The depth of the adder structures is reduced on the basis of generating the carry signals in parallel form. This property is the main

All articles published in Journal of Electrical Engineering and Electronic Technology are the property of SciTechnol and is protected by copyright laws. Copyright © 2023, SciTechnol, All Rights Reserved.

advantage of these adders. The structural details of the existing bit parallel prefix adders. The sklansky adder has suitable hardware and time complexities compared with the others. Therefore, here, we use this adder for implementing the modular adder in the Speck block cipher.

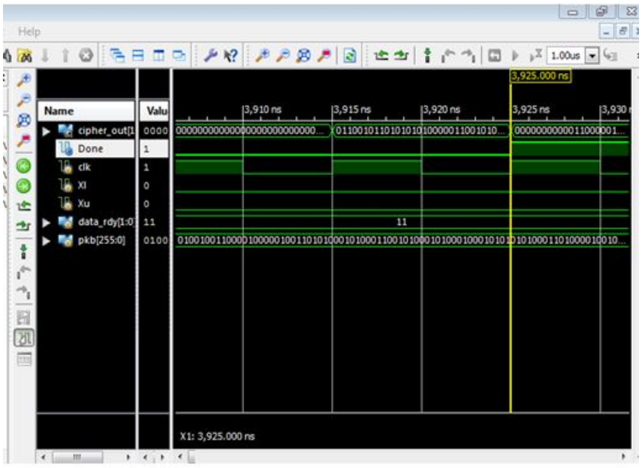
Results

The results of the proposed implementations and other related works on Speck cipher are that indicates the critical path relay of the existing work and the proposed work of the Simon and Speck block cipher using flexible architecture. This is light weight block cipher to reduce the critical path delay to perform the encryption and decryption operation. It is most useful methoda.



```
=========================================================================
Timing constraint: Default OFFSET OUT AFTER for Clock 'clk'
  Total number of paths / destination ports: 7 / 7
-------------------------------------------------------------------------
Offset:              5.969ns (Levels of Logic = 2)
  Source:            roundcnt_5 (FF)
  Destination:       rndlessthan32 (PAD)
  Source Clock:      clk rising

  Data Path: roundcnt_5 to rndlessthan32
                                Gate     Net
    Cell:in->out      fanout   Delay   Delay  Logical Name (Net Name)
    ----------------------------------------  ------------
     FDRE:C->Q            28   0.514   1.072  roundcnt_5 (roundcnt_5)
     INV:I->O              7   0.612   0.402  rndlessthan321_INV_0 (rndlessthan32_OB
     OBUF:I->O                 3.169          rndlessthan32_OBUF (rndlessthan32)
    ----------------------------------------
    Total                      5.969ns (4.295ns logic, 1.474ns route)
                                       (72.0% logic, 28.0% route)

=========================================================================


Total REAL time to Xst completion: 9.00 secs
Total CPU time to Xst completion: 9.16 secs

-->
```

```
==========================================================================

Process "Synthesize - XST" completed successfully
```



Conclusion

The proposed structures are implemented on the proposed structures for Simon; the XOR operations are implemented on the basis of a tree structure for reducing critical path delay. In addition, we proposed flexible structures that can perform various configurations of the Simon ciphers supporting variable key and block sizes. Therefore, the flexible architectures provide versatile implementations with adaptive security level and the ability of encryption of longer messages based on variable key size and variable block size.

The implementation results show that the proposed structures have better performance in terms of critical path delay compared with other existing works. The result analysis are compared and verified by using Xilinx ISE 14.2 software tool. The future work is implemented by using Speck block cipher with add one adder to reduce the delay and power at the output side.

References

1. Yang X, Dai Z, Zhang Y, Yu X (2008) The research and design of reconfigurable computing for Block cipher. J Electron (China) 25:503-510.
2. Pandey JG, Goel T, Karmakar A (2019) Hardware architectures for present block cipher and their FPGA implementations. IET Circuits Devices Syst 13:958-969.
3. Rashidi B (2020) Efficient and flexible hardware structures of the 128 bit clefia block cipher. IET Comp Digital Techn 14:69-79.
4. Artiles JA, Chaves DP, Pimentel C (2019) Image encryption using block cipher and chaotic sequences. Signal Process Image Commun 79:24-31.
5. Li G, Xu J, Dai Z, Wang S, Zhu Y (2017) A flexible data scheduling scheme for block cipher processor. Procedia Comput Sci 107:395-400.
6. Dinu D, Corre YL, Khovratovich D, Perrin L, Grobschadl J, et al. (2019) Triathlon of lightweight block ciphers for the internet of things. J Cryptogr Eng 9:283-302.