Implementation of SIMON & SPECK Algorithm

*1 Anil G. Sawant,2Sayali Kamthe, 3Yashasvini Shaha , 4Bapu Morajkar , 5Abhishek Sakpal
*1 Research Scholar (Asst. Professor) ,2Student, 3Student, 4Student, 5Student
*1 JJT University, Rajasthan, India (Trinity College of Engineering and Research, Pune), 2 Trinity College of Engineering and Research, Pune , 3Trinity College of Engineering and Research, Pune, 4Trinity College of Engineering and Research, Pune, 5 Trinity College of Engineering and Research, Pune.

Email:* anilsawant.22@gmail.com, sayalikamthe16@gmail.com, yashasvinishaha01@gmail.com,bapumorajkar@gmail.com, abhisakpal42@gmail.com.

Abstract **-** Nowadys, the security of exchanging information and communication such as authentication and privacy are essentially important. Cryptographic algorithms such as block ciphers and stream ciphers are basic components for security. Security, simplicity and flexibility are the conflicting goals in the cryptographic design. The speck and Simon families of block cipher are designed specifically to offer security on the constrained devices, where the simplicity of design is important. Simon and speck, each of this comes in a variety of widths and key sizes. Moreover, it is also reduces the inefficiency of encrypting slightly longer messages by supporting a variable block-size. Many lightweight block ciphers were designed to perform well on a single platform and were not meant to provide high performance. while, Simon and speck each provide or offers excellent performance on hardware and software platforms, is flexible enough to admit a variety of implementation on variety of platforms and is easy to analysis using existing techniques. Both perform exceptionally well across the full spectrum of lightweight applications, but the Simon is tuned for optimal performance in hardware, and the Speck for optimal performance in software. In our project, we analysis the "Simon and speck" block cipher family and then simulate and synthesize this algorithm. We are going to implement the "The Simon and The Speck "the cryptography algorithm on a FPGA.

Keywords-Cryptographic algorithm, block cipher, FPGA.

Introduction:

In today's world while communicating through an untrusted media or network such as internet it is necessary to keep the system secure, The cryptography is the study of techniques which can used to protect secrets and secure personal information. with the help of encryption and decryption technique one can secure their communication and data in presence of enemy[1][7]. Cryptography further classified into two categories: symmetric and asymmetric key. Here we have to study a block cipher SIMON & SPECK algorithm along with a symmetric key to encrypt and decrypt a block of data rather than the one bit at a time[1]. Before studying the SIMON & SPECK algorithm there should consider the drawbacks of previously used algorithms[2]. The AES block cipher is one of the most used block cipher, ASIC implementation of AES 128 developed with an area of just 2400 gates equivalents and the fast software implementation is available For 8 bit and 16 bit microcontrollers[6][7]. However they tends to fall short of what is required for today's constraints environment and so wont meets futures requirements or needs. The AES implementation on microcontrollers is fast but they tends to be large in size and complex also. The small implementation in AES tends to complex one and also slow. There are the some reasons for developing the new lightweight block ciphers[3][6]and like AES many block ciphers are proposed i.e. two-fish algorithm ,present algorithm etc.

Traditional cryptography not well suited for computational task perform on smaller devices. We proposed light-weight cryptography to perform well on various constrain platforms. SIMON and SPECK are invented in publically on JUNE 2013 by NSA (National Security Agency). In this we propose highly optimize and secure block cipher ,SIMON& SPECK[1] that are much flexible which can gives us a excellent performance on hardware and software [4][5][8]. In terms of memory usage and code size it gives best comparable software algorithm and in terms of throughput it gives best comparable hardware implementation. The both algorithms Simon and speck provide the flexibility across various platforms and perform well in both software and hardware , while SIMON has optimize for performance on hardware devices and speck for software . The both SIMON & SPECK algorithms are available in different block sizes and different key sizes which admits variety of implementation in order to provide flexibility SIMON & SPECK supports block sizes of 32,48,64,96 and 128 bits with up to 3 key sizes. Each family provides different algorithms in all. list of different block sizes and key sizes in bits are:

Block size	Key sizes
32	64
48	72,96
64	96,128
96	96,144
128	128,192,256

Table 1: Simon & speck parameters

SIMON Family of Block Cipher:

Simon is lightweight balanced Feistel block ciphers published by NSA, for high performance in hardware it can be implemented software also. Simon proposed to growing need for flexible, secure and lightweight cryptography[1]. SIMON block cipher with the 2n/bit block and the mn bit key is denoted SIMON 2n/mn . Where n should be 16,24,32,48 or 64 and m should be 2,3,4 . Here we will evaluate SIMON family of block ciphers i.e. SIMON64/128. Our aim to design SIMON to obtain the lightweight round functions which provide more security. The SIMON cipher is symmetric block cipher algorithm with a features like simple mathematical computations, yet secure, round function that provide security and design in various power constraints environments. SIMON is bit-based algorithm. For encryption and decryption maps use a following operations on n-bit word:

- Bitwise XOR,
- Bitwise Adding,
- Bitwise left and right circular shift.

SIMON Round Function:

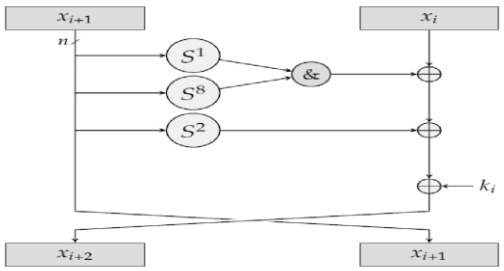

Fig 1: simon round function

The SIMON to n round function is the map ,Rk,defined by,

Rk(x,y) ->(y xor f(x) xor k,x)Where;k is a round key,x and y are xi and xi+1 respectively and F(x)= (Sx&S^8x)xor S^2x .The inverse of round function used for decryption.

Above figure shows the round function of SIMON,xi+1 and xi denotes the upper and lower words of block which is a n bit word. These two words holds the initial input which is called a plaintext. As round function consist of bitwise ANDing, bitwise XORing and left circular shift operation ,In every round circular left shifting and bitwise AND operation are perform on the xi+1 i.e. upper word and it is XOR with xi i.e. lower word and the round key. The resulting value is written as a upper word while its content is transferred over to the lower word. The round functions are continues to run repeatedly until the desired number of rounds are reached in our case the round function count is 44.In case of SIMON block cipher decryption is exact reverse structure of encryption.

The round keys are generated a number of times that is a function of block and key size, shown below:

Block size 2n	Key size mn	Word size n	Key words m	Constant seq	Rounds T
32	64	16	4	Z0	32
48	72 96	24	3 4	Z0 Z1	36 36
64	96 128	32	3 4	Z2 Z3	42 44
96	96 144	48	2 3	Z2 Z3	52 54
128	128 192 256	64	2 3 4	Z2 Z3 Z4	68 69 72

Table 2: Simon round function

Key Expansion:

As there are number of round functions in SIMON family. SIMON block cipher needs unique key for each round function. These round keys are generated by keys expansion function. There are 3 related key schedules, depending on the number of key words 2,3 and 4. The key schedules produce round keys k0,k1,k2,k3……from a key values k0 to km-1,where m should be 2,3 and 4. for SIMON 64/128 the key schedule is 4.The SIMON key schedules use one of the five sequence Zj(j=0,1,2,3,4).

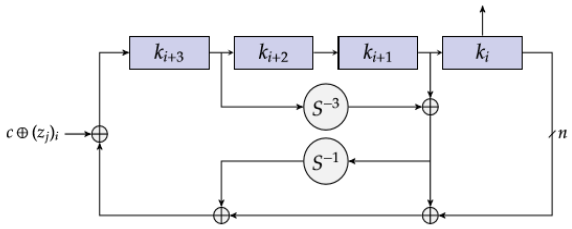

Fig 2: key expansion

Let c = 2n − 4 = (2n – 1) XOR 3 = 0xff · ·· fc. For Simon2n with m key words (km−1. . . k1, k0) and constant sequence z3, round keys are generated by

Ki+4 = ki XOR (I XOR s^-1)(s^-3 ki+3) XOR Ei

Where,Ei is round constant.

SPECK Round Function:

SPECK is an"ARX"(Add,rotate,xor)design. The speck has been designed to provide excellent performance in both hardware and software, but have been optimize better performance on software. The notation for SPECK is analogous to SIMON[1][2]. The SPECK 2n encryption maps make use of the following operations on n bit word:

- Bitwise XOR
- Modular Addition
- Left and right circular shift

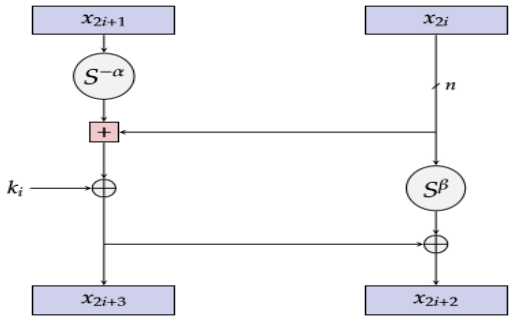

Fig 3: Speck round function

The encryption round functions of SPECK light-weight block cipher consist of bitwise XOR operation, addition modulo 2 operations, left and right circular shift operation. In case of round key, it can be expanded by key schedules. The round function will operate round number (T) time according to SPECK block cipher parameters. The key dependent SPECK 2n round function is map Rk:

Rk(x,y) = ((S^−α x+ y)⊕k, S^β y⊕(S^−α x+ y)⊕k)

Where α=8 and β=3 And the reverse structure of the round function ,necessary for decryption.

Parameters for different versions of SPECK are:

	Key size mn	Word Size n	Key words m	α	β	Rounds T
32	64	16	4	7	2	22
48	72 96	24	3 4	8	3	22 23
64	96 128	32	3 4	8	3	26 27
96	96 144	48	2 3	8	3	28 29
128	128 192 256	64	2 3 4	8	3	32 33 34

Table 3: speck parameter

The SPECK key schedules take a key and from it generate a sequence of T key words k0....kT−1, where T is the number of rounds. The efffect of the single round function Rki is shown in above table

Related algorithm comparison:

		Hardware		software	
size	**name**	**Area (GE)**	**Tput (kbps)**	**Flash (bytes)**	**Tput (kbps)**
48/96	Simon	763	15.0	196	589
	Speck	884	12.0	134	943
	EPCBC	1008	12.1	365	93
64/128	Simon	1000	16.7	282	515
	Speck	1127	13.8	186	855
	Present	1339	12.1	487	96
96/96	Simon	984	14.8	454	454
	Speck	1134	13.8	276	866
	EPCBC	1333	12.1	730	93
128/128	Simon Speck	1317	22.9	732	342
	AES	1396	12.1	396	768
		2400	56.6	943	445

Table 4: algorithms comparison

Conclusion:

SIMON & SPECK Algorithm is a lightweight flexible algorithm. Due to the flexibility of algorithm used in various applications and environments, data and key length can be selected with different sizes. This flexibility is a consequence of the simplicity of the design and this simplicity of Simon and speck is additionally benefits. they are very easy to implement and efficient implementation can be had for minimal work this is contrast to the situation for algorithms such as AES.Simplicity makes the algorithm attractive target for cryptoanalysis.The approach we have taken to design lightweight block cipher Simon and speck algorithm means they will continue to offer high performance on future's IoT devices.

References:

[1] Ray Beaulieu, Douglas Shors , Jason Smith, Stefan Treatman-Clark, Bryan Weeks, Louis Wingers, "The Simon and Speck of lightweight block ciphers," National Security Agency 9800 Savage Road, Fort Meade, MD 20755, USA, JUNE 2013.

[2]]C. D. Cannière, O. Dunkelman and M. Kneževi´c, "KATAN and KTANTAN - A Family of Small and Efficient Hardware-Oriented Block Ciphers,"Springer-Verlag, 2009 [In CHES 2009, the Lecture Notes in Computer Science No. 5747, pages 272–88.]

[3] Kyoji Shibutani, Takanori Isobe, Harunaga Hiwatari, Atsushi Mitsuda, Toru Akishita, and Taizo Shirai, "Piccolo: An Ultra Lightweight Blockcipher," Sony Corporation 1-7-1 Konan, Minatoku, Tokyo 108-0075, Japan, 2011.

[4] M. Zwolinski, "Digital System Design with VHDL,"2nd Edition, 2004.

[5] Giovanni De Micheli, " Synthesis and Optimization of Digital Circuits," 1994.

[6] Ehsan Vahedi,Vincent W.S. Wong, Ian F. Blake, "An Overview of Cryptography," Chapter 5,The University of British Columbia, Canada, 2014.

[7] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, "Handbook of Applied Cryptography", CRC Press, August 2001, PP. 202-203.

[8] Xilinx, Inc., Virtex-5 User Guide, Available At www.xilinx.com.