International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Skein and Threefish Implementation on FPGA

Litty.P.Oommen[1], Anas A S [2]

[1]P G Scholar, VLSI and Embedded Systems, Dept. of ECE, T K M Institute of Technology, Kollam, India

[2]Assistant Professor, Dept. of ECE, T K M Institute of Technology, Kollam, India

Abstract*: Hash functions are commonly used in the cryptography for providing security. SHA1, SHA 2 etc are some hash functions. These SHA variants can be replaced with Skein. Skein is a hash function which is built from the tweakable Threefish block cipher. The basic building blocks of Skein are Threefish block cipher, Unique Block Iteration and an Optional argument system. The use of tweakable block cipher allows skein to hash configuration data along with the input text in every block. A coprocessor for Threefish architecture can be designed. The different steps for building hash function are Key Schedule, Threefish encryption and Skein Hashing. For Skein 256, both the keyword and plain text should be of 256 bits. Key schedule is used for the generation of subkeys, which can be used for the encryption process. Skein hash function can be computed using the Threefish block cipher which is the output of encryption process. The advantage of Skein over other SHA3 finalists is that it allows both hashing and the encryption. The VHDL coding for Key Schedule and Threefish encryption have done. The subkeys which are the output of Key Schedule and Cipher text which is the output of threefish encryption were simulated using Modelsim 6.3f.*

Keywords: UBI, Threefish block Cipher, FPGA, Hash function, Skein

1. Introduction

Cryptography is the study of and the practice of techniques for providing secure communication in the presence of third parties. Some applications of cryptography are authentication, privacy, integrity and non- repudiation[3]. The three types of cryptographic algorithms are Secret key cryptography, Public key cryptography and Hash functions. In secret key cryptography, same Key can be used for both the encryption and decryption process. In public key cryptography, one key can be used for encryption and the another key can be used for decryption process. Cryptograhic hash function is a transformation that takes an input (message) and returns a fixed size, alphanumeric string. Values return is called hash value[4]. Hash functions gained a high level of importance in data traffic. Cryptographic Hash function takes a string of arbitrary length input and maps it to a fixed length output string.The cryptographic hash function Skein can be built from the tweakable threefish block cipher[1],[2]. Skein is a cryptographic hash function which is available in three internal state sizes such as 256, 512 and 1024 bits. The main components of Skein are Threefish Block Cipher, Unique Block Iteration and an Optional Argument system[6].The Threefish Block Cipher is the core of the Skein. Skein allows both the hashing and encryption in same co-processor.

2. Methodology

Skein Hash function can be built from the Threefish block cipher. The initial step is to generate the sub-keys from Keyword and the tweak word which are the inputs. For Skein 256, the plain text and keywords are of 256 bits. The tweak is of 128 bits. The Next step is the threefish encryption process. For the encryption process, 72 rounds have to be completed. The decryption is the reverse operation of encryption. The output of the threefish encryption is the Cipher text. Using that threefish block cipher and Unique Block Iteration, Skein hash function can be computed. Skein allows hashing and encryption in the same co-processor.

3. System Overview

The basic block diagram for Skein is shown in Figure1.

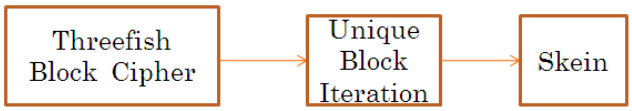

Figure 1: Block Diagram of Skein

The Skein hash function can be built by using Threefish Block Cipher and Unique Block Iteration.

3.1 TheThreefish Block Cipher

The Threefish block Cipher works on the principle that, ”a large number of simple rounds is more secure than the fewer complex rounds”. The threefish operates on unsigned 64 bit integers. It involves three operations. The three operations in threefish are:

- Rotation of k bits to the left.
- bit wise exclusive OR.
- Addition

The threefish block cipher is a tweakable block cipher. Different number of rounds are required for different key sizes of threefish. The number of rounds for different key sizes of threefish is as shown in the figure 2.For Skein 256, the number of words is 4 and the number of rounds required are 72 rounds.

Block/Key Size	# Words N_w	# Rounds N_r
256	4	72
512	8	72
1024	16	80

Figure 2: Number of rounds for different key sizes of threefish

The plain text is represented as 'P' and Key is represented as 'K'. Both the Plain text and Key are converted into Nw 64 bit words. For Skein-256, the value of Nw is 4.Number of rounds, Nr is 72 and block size Nb is 32 bytes. The Plain text and Cipher key are represented as the combination of four 64 bit words. The number of words Nw and the number of rounds Nr depends on the Key-size. The size of a plain text block is given by Nb =8*Nw bytes.

3.1 Key Schedule of Threefish

The function of Key Schedule is to generate the subkeys from a block Cipher key and a Tweak The key is of 256 bits and tweak is of 128 bits. Key is represented as (K0,K1,K2,K3) and the tweak is represented as (t0, t1). For Skein 256,since the value of Nw is 4, Key is expressed as (K0,K1,K2,K3) . There are three inputs for the Key Schedule. They are
a)Block Cipher Key K=(K0,K1,K2,K3)
b)a tweak T=(t0,t1)
c) ConstantC240= 1BD11BDAA9FC1A22

Tweak:The purpose of tweak is to make each block operation in Skein unique.

Constant C240 :The constant C240 defends against generating extended Keys which are all zero or almost zero. It ensures that extended key cannot be all zeros. It also provides an additional defence against rotational attacks. C240 is the AES encryption of the Plain text 240(in decimal) under the all zero 256 -bit key. C240 =AES-256(240).

The key schedule starts by defining two additional words, K4 and t2. The first step of Key schedule is the extension of Key Word and the tweak word. Key word can be extended by exoring different words (K0,K1,K2,K3) with constant C240 .

K4 = C240 xor K0 xor K1 xor K2 xor K3…..(1)

The extended tweak word t2 can be done by XOR ing t0 and t1.

t2 = t0 xor t1…… (2)

Then the subkeys Ks=(Ks,0,Ks,1,Ks,2,Ks,3)are defined by:

Ks,0 = K(s+i)Nw+1for i = 0,….Nw - 4 …….(3)

Ks,1 = K(s+i)mod(Nw+1) + ts mod3 for i = Nw – 3 ….. (4)

Ks,2 = K(s+i)mod(Nw+1) + t(s+1)mod3 for i = Nw -2 (5)

Ks,3 = K(s+i)mod(Nw+1) + s for i = Nw - 1 …..(6)

where 0<=s <= 18. Therefore the output of Key Schedule is the 19 subkeys

3.2 Threefish Encryption

In the case of Skein 256, 72 rounds have to be performed to complete one encryption process. Four of the 72 encryption rounds of threefish 256 is as shown in the figure 3. In Threefish encryption, the subkeys are injected only at the interval of 4 rounds.

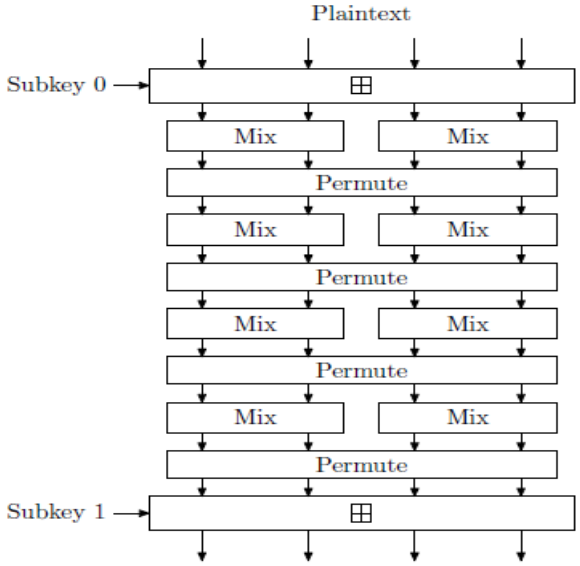

Figure 3: Four of the 72 rounds of threefish encryption

Plain text is added with the subkeys only when the condition is that d mod 4=0, where d indicates that which round is performing. Two MIX operations and one permute operation together constitute a round. Similar 72 rounds have to be performed to complete one encryption process.

MIX Function

MIX is a nonlinear mixing operation. It operates on two 64 bit words.Function MIXd,j has two input words (x0,x1). It produces two output words (y0, y1). It can be obtained by two relations.

$y0 = (x0 + x1) \bmod 2^{64}$……(7)

y1= (x1 << R(dmod8),j) xor y0) where << is the rotate left operator.

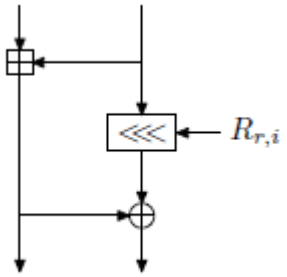

Figure 4: MIX function

The Rd,j constants are shown in the figure 5 given below.

N_w		4		8				16							
j		0	1	0	1	2	3	0	1	2	3	4	5	6	7
	0	14	16	46	36	19	37	24	13	8	47	8	17	22	37
	1	52	57	33	27	14	42	38	19	10	55	49	18	23	52
	2	23	40	17	49	36	39	33	4	51	13	34	41	59	17
$d=$	3	5	37	44	9	54	56	5	20	48	41	47	28	16	25
	4	25	33	39	30	34	24	41	9	37	31	12	47	44	30
	5	46	12	13	50	10	17	16	34	56	51	4	53	42	41
	6	58	22	25	29	39	43	31	44	47	46	19	42	44	25
	7	32	32	8	35	56	22	9	48	35	52	23	31	37	20

Figure 5: Round constant Rd,j for each Nw

Permute function

The output of the word permutation is the output of each round. The detailed diagram for threefish encryption is as shown as figure 6.

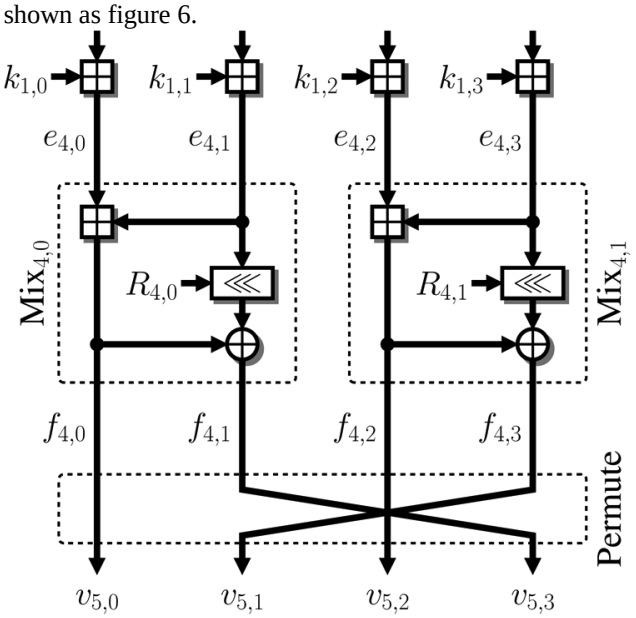

Figure 6: Threefish encryption

The Key Schedule turns the key and tweak into a sequence of 19 subkeys, each of which consists of Nw words. The words of subkey is denoted by (Ks,0,Ks,1,Ks,2,Ks,3). Assume that, Vd,i be the value of i^{th} word of encryption state after d rounds. Initially,V0,i= Pi, for 0,...3.and then apply Nr rounds numbered d=0,...Nr-1. For each round ,add a subkey if d mod 4=0.

For i=0,...3 ed,i = f(Vd,i + Kd/4,i)mod2^{64} ifdmod4 = 0 …(9)

ed,i = Vd,i otherwise ….(10)

The Mixing and permutations are defined by:

(fd,2j ,fd,2j+1) = MIXd,jed,2j ,ed,2j+1 for j = 0, …(11)

From the figure of threefish encryption, it is clear that plain text is added with subkeys only when d mod 4=0. Then Perform the Mixing and Permute operations. Each mixing operation is the combination of addition ,left rotation and an exclusive OR operations. The order of permute function when Nw= 4 is 0,3,2,1. The fd,i values are the results Of MIX function and output of the word permutation is the output of the round. The cipher text C is given by

Ci = (VNr,i + K18,i)mod26 ……(13)

3.3 Threefish Decryption

The threefish decryption is the reverse process of threefish encryption. The diagram of threefish decryption is as shown in the figure. Here, Subkeys are used in the reverse order. Cipher text is the input of the threefish decryption. Then perform the permute and the inverse MIX operation. Inverse MIX operation consists of an exclusive OR,right rotation and 64 bit subtraction. Then subtraction operation is performed between the subkeys and the cipher text, only when d mod 4=0. The output of the threefish decryption process is the plain text. The diagram of threefish decryption is as shown in Figure 7

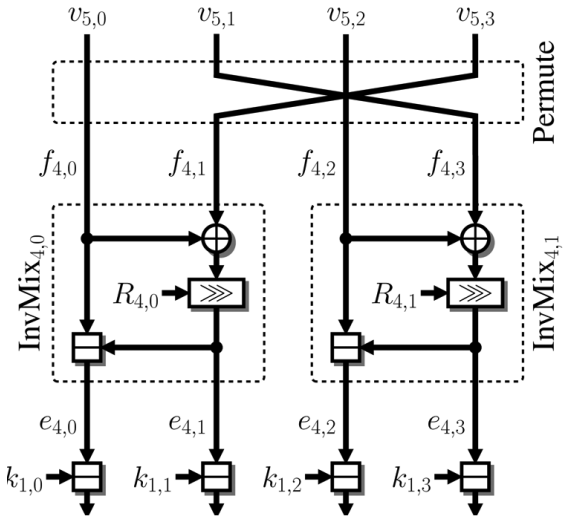

Figure 7: Threefish decryption

3.4 Skein Hashing

The Unique Block Iteration (UBI) chaining mode allows one to build a compression function out of a tweakable encryption function E(T,K,P) . Let M be a message of arbitrary length up to 299 8 bits. If the number of bits in M is not a multiple of 8, append a bit 1followed by a (possibly empty) string of 0s. This step guarantees that M contains N_M bytes. Then,pad M with p zero bytes so that N_{M+p} is a multiple of block size N_b.M can be splitted into N_b byte blocks M,… $M_{\beta-1}$, where $\beta = (N_{M+p})/N_b$. Each block Mi is processed with a unique tweak value Ti encoding how many bytes have been processed so far, a type field and two bits specifying whether it is the first and or last block. The UBI chaining mode is computed as,

H0 ← G ……..(14)

Hi+1 ← Mi xor E(Hi,,Ti,,Mi)….. (15)

where G is a starting value of N_b bytes.Skein is built on three invocations of UBI:

- Define a 32-byte configuration string that contains the length of the digest size(in bits), a scheme identifier, and a version number. Compute the N_b byte block G_0 as $G_0 \leftarrow UBI(0,C,T_{cfg}2^{120})$ on the digest size and can be pre computed. The message is then processed as follows :
- A third call to UBI is required to achieve hashing appropriate randomness

$H \leftarrow UBI(G1,0,T_{out}2^{120})$

4. Results and Discussions

The modules are modelled using VHDL in Xilinx ISE Design Suite 12.1 and the simulation of the design is performed using Modelsim SE 6.3f to verify the functionality of the design. Here a structural model is used for the coding purpose. Key schedule, threefish encryption and Skein hashing are the various steps in Skein hashing. The VHDL coding for key schedule and threefish encryption have done. Then these blocks were simulated using modelsim 6.3f.The simulation result of Key Schedule module is as shown in the figure 8.

The Key Schedule generates 19 subkeys using Key word and tweak word. The input of the Key Schedule module is 64 bit Key word and 128 bit tweak word. The output is the combination of 19 subkeys. Subkeys are represented as Ks0,Ks1,Ks2,Ks3.The value of s varies from 0 to 19.Subkeys are generated by adding extended Key word and tweak word.

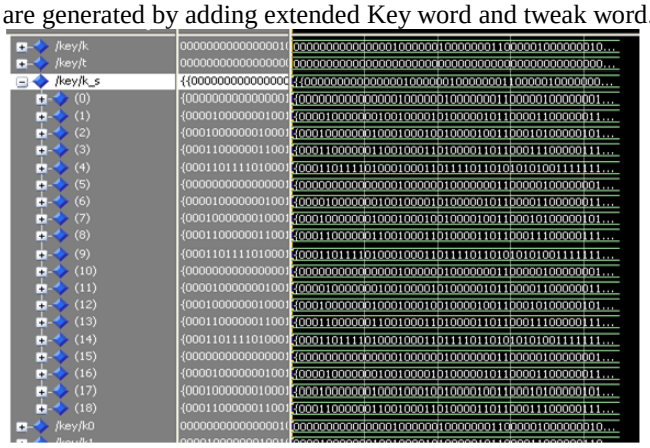

Figure 8: simulation result of key schedule

The input of threefish encryption is plain text, key word and tweak word. Plain text is of 256 bit,Key is of 256 bits and tweak is of 128 bits. The output is Cipher text C is of 256 bits. The simulation result of threefish encryption is as shown in figure 9.

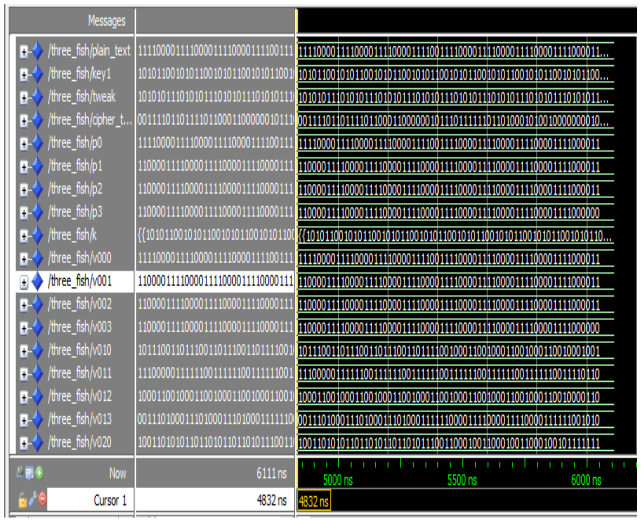

Figure 9: simulation result of threefish encryption

5. Conclusion

Skein is a good replacement of SHA family. Skein is an efficient tool to be used for large number of functions due to its optional and extendable argument system . It is efficient for both hardware and software platforms. Skein can be built using Threefish block Cipher. Subkeys have been generated using Key Schedule. Extended Key word and tweak word are added to get subkeys. Threefish encryption was performed to generate the cipher text. Plain text was added with the subkeys to generate cipher text.

References

[1] Nuray At,Jean-Luc Beuchat,Eliji Okamoto,Ismail San and Teppei Yamazaki,"Compact hardware implementations of Chacha,Blake,Threefish and Skein on FPGA",IEEE Transactions on Circuit and Systems, vol. 61 ,no.2,February 2014.

[2] N.At,L,Beuchat, and I,San"Compact implementation of threefish and skein on FPGA",in Proc. ITIP, 2012.

[3] WilliamStallings,"Cryptography and Network security principles and practices".

[4] Seminararbeit,Timo Bartkewitz,"Building Hash Functions from Block Ciphers,Their security and Implementation Properties" Ruhr-University Bochum.

[5] Sivasankari.S.A,Allan Mary George,Pavitra .S "The Skein Hash function,"Int.Journal of Engineering Research and Applications. Vol. 3, Issue 6, Nov-Dec, 2013.

[6] N.Ferguson,S.Lucks, B. Schneier, D.Whiting, M.Bellare,T. Kohno, J. Callas"Skein Hash function family".