Cryptanalytic JH and BLAKE Hash Function for Authentication and Proposed Work Over BLAKE-256 Using C

Mr. Somil Jain¹, Jagannath University, Jaipur(Raj.), INDIA,

Mr. Vaibhav Doshi², Amity University Rajasthan, Jaipur(Raj.), INDIA,

Mr. Tarun Goyal³, SIET Rajasthan, Sikar(Raj.), INDIA,

Abstract: Hash functions form an important category of cryptography, which is widely used in a great number of protocols and security mechanisms. Hash functions are a fundamental primitive category of security science. It is defined as computationally efficient function, which maps binary strings of arbitrary length to binary strings of fixed length. The last ones are the outputs of a hash computation and they are called hash values. Hash functions are applied to support digital signatures, data integrity, random number generators, authentication schemes, and data integrity mechanisms. National Institute of Standard and technology (NIST) has selected the 14 Round Candidates of SHA-3 Second the Competition. It focus on the new SHA-3 competition, started by the NIST, which searches for a new hash function in response to authentication concerns regarding the previous hash functions SHA-1 and the SHA-2 family.

This work is based on comparative study of two SHA-3 cryptographic hash function candidates JH and BLAKE (out of fourteen). It compares the common features of both candidates which is widely used in above mentioned applications and improvement over SHA-256 with proposed work BLAKE-256 hash function.SHA-256 is used 64 rounds to calculate 256 bit final hash value with 256 bit initial hash value but BLAKE-256 is used 14 rounds to calculate final hash value with same input length and same output length. **Keyword:** SHA-3, JH ,BLAKE , Hash, Compression Function.

INTRODUCTION

We proposed a new compression function structure to construct a compression function of JH from a block cipher with constant key. JH compression function is constructed from a bijective function (a block cipher with constant key) [4]. The block size of the block cipher is 2m bits,2m-bit hash value H⁽ⁱ⁻¹⁾ and the mbit message block M⁽ⁱ⁾ are compressed into the 2m-bit H⁽ⁱ⁾. The BLAKE family contains four hash functions: BLAKE-28, BLAKE-32, BLAKE-48, BLAKE-64, with the bit lengths of their digests being 224,256,384 and 512, respectively. The former two operate on 32-bit words, while the latter two work with 64-bit words [3]. BLAKE comes in two variants: one that uses 32-bit words, used for computing hashes up to 256 bits long, and one that uses 64-bit words, used for computing hashes up to 512 bits long.

Compression Function is the main core of the hash functions data transformations, for a certain number of rounds for each hash function.

The compression function of BLAKE-256 takes as input four values [3]:

- 4 Message block $m = m_0, \ldots, m_{15}$
- $4 Salt s = s_0, \ldots, s_3$
- $\mathbf{4} \quad \text{Counter } \mathbf{t} = \mathbf{t}_0, \, \mathbf{t}_1$

These four inputs represent 30 words in total (i.e., 120 bytes = 960 bits).

The output of the function is a new chain value $h'=h'_{0,...,}h'_7$ of eight words (i.e., 32 bytes = 256 bits). We write the compression of h, m, s, t to h' as

h' = compress(h, m, s, t)

COMPARATIVE STUDY OF JH AND BLAKE

FACTOR	ш	BLAKE
Strutae	Destive	HAIF msle
Hish variants	Single design	Two variants
Tipe	Block cipher hoved	Add-XOR-Ratate
Restart to length extension	Exch message Nock is 64 lyter	Message length limited to respectively 2 ⁴⁰ and 2 BLAKE-256 and BLAKE-512
Interface	Interfacing with initial values	Interfacing with sult
Security	Enty to molyre and large security margin	Bood m intensively based component/ClaCi resistant to generic second-preimage attacks
Performance	Efficiently implemented, simple component and lagis parallelizability	Fast in both software and hardware, parallelism a flamgingerizers
Fast is both software and hardware	16.3 cycles/hyte az 64 hit care 2 microprocessor, 21.3 cycles/hyte az 32 bit core 2 microprocessor Bit-skor, statoble for 128 bit SDAD astruction at	latel core 2 Dav.BLAKE-255 can hold at about cycle-byte and BLAKE-912 can hold at about cycle-byte
Politing science	1.0% mml suggemt/3Handf125 125 bit messagelength mm 512 bits added	1.0% until congruent/441mod912).64 hit mesot length for HEAKE-224 1.0% well congruent/447mod912(1).64 hit mesot length for BEAKE-256 1.0% until congruent/941mod1024(128 hit mesot length for BEAKE-384 1.0% until congruent/941mod1024(1,128 hit mesot length for BEAKE-1024

Table 1. Comparative Results of JH and BLAKE

SIMULATION WORK

It gives us C code computing the compression function of BLAKE-256.

Initialization

It calculates initialization step of BLAKE-256 with the input of initial chain value (hxdi), salt (sxdi) and counter (txdi) and generate state value (vxdo).

• Round Function

It calculates round function step of BLAKE-256 with the input of state values (axdi, bxdi, cxdi,

dxdi), message word (mxdi) and constant word (kxdi) which is generated by initialization step of BLAKE-256, and then it generate new state values(axdo, bxdo, cxdo, dxdo).

• Finalization

It calculates finalization step of BLAKE-256 with the input of final state values vxdi (which is generated after 14 round), salt (sxdi), initial chain value (hxdi) and then it generate final chain or hash value (hxdo).

It gives us C code computing the compression function of BLAKE-256 with Header File BLAKEh.h and Turbo file Turbo.c.

Firstly, It calculates G₀(v₀, v₄, v₈, v₁₂)

😰 Turbe C++ DE	. D x
Received the	
two-black nessage:	
HLAXE-32 Doory 385 doorf yeedoodd 39 2000065 Franklonds 22 radiaes ar candeldy 31 adabet 666	
HLAKE-28 Books-concenses/Inconcensif44000ker350000kee72000akes33300000kee15	-
RL&XE-54 Broomenseerers 71 Herreererererer 1 Herreererererererererererererere Broomenseerer 71 Herreererererererererererererererererer	00152
ELEXE-48 Bereformennes (540ennennenneter) nemmennen (5510ennennen) Bereformennen (55	194205

Figure1: Hash values Obtained after Two Block Message

International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue 6–June 2013

an Tarte Crit 01	. 01	
STORING TO A CONTRACT OF A CONTRACT	and and a state of the	
tar-block warraget		
TLANE->2 00007 18x000874 E100001011 20000674 n 000853 23 N05005 An C0600107 11 A000C36.6		
ELANE-28 ERSEC CONSISTATION OF FINISHING AT ANY INSTITUTION TO THE REPORT OF		
ELZ (2) – 6.4 andarisko karikante (15.7), ile neorosko karika (17.), v processi zakonala (17.) verska karikana karika (17. 4 karika karika zakona karikana karika (18. karika karika karika (17.) zakona karikana karika (17. 4. 5)	HINNCIST	
ELANET - M Managementanya (12) - Managementanya (Kanagementanya), 151 mentangkanya (Managementanya) Managementanya (Kanagementanya), 163	02604025	
nu-hloch surrays (
ELANE - 32 Nikologi 32900007/52200000003/900000000700000529/000006591100000075600000000		
NTANI. 28 Normal Al-Arikenti (Y2 Norma) 71 yonnaliyo donorman tatariki 44 yongor Firi		
NEA MER - 6.4 International and a second second International second	99990 COC	
12.6.12 ⁻⁰¹ 1999 - 1999 - 1997 - 1999 - 199 - 1999 - 1 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 199	*****	

Figure2: Hash Value Obtained After one-block message



Figure3 : Changed Hash Value After Two Block-Message



Figure4: Changed Hash Value After One-Block Message

and Turbo C++ IDE	- C X
AND DESCRIPTION OF THE PARTY OF	
tun-bloch nessaget	
DLANE-32 Nextor a 430004965 L FORMACDY FORMA	DLTS ANNUES 2 D-MANNAES, D TO ANNAED VIET WINNER CO.DV.
01.6 KT-28 00006-CU1 0000643400000713E0000	06470000043000015580000472C
	PE1 94060806000000007 7406008060000000000000000000000000000000
BLAYE-48 Markenson (C24000000000000000000000000000000000000	2017 CARGONARDONANG 15 1 PORTONONING 7 196 INFRANTONING DAIP.
one-block message?	
RLANS - 12 HERBELAG FORMANT TOMOURS 17 DAIWAR	LVASEBBBS2E48808687398880V1888860555
BLANE-28 RENERCAL DEBUGAL DE DEMONSS 26 ANEXE	0-406-500-00079 1-60-0011 5-47-000-001 77C
BLAKE-64 Newskiesterster, D. Charlestersterster Newskiestersterster 127 December State	6.1 PLONMARKANANANANCO 4000000000000000000000000000000000000
51.4X2-48 10000000000007114298000000000000000000000000000000000000	CD 101000000000007075.000000000000007461.00000000000000000
two-block menaget	
NLANE-32 Newska 4 Skiennik i Krieger Dy Kriege	01758888521-88886681088094788888C006
8LAN3-28 Mellon Cit 20000n 436 00007 13 E0000	060 Y000000 K300001 S5600000 P2C
ILAYE-64 Distant Constant?: 7: 000/00/00/00/00/00 Distant Constant Constant Constant	FE 1 YERERANDORDER YHDERDRENDREN FE HEIRERANDORDER 152 YEE DRINNINGHRUNDES H 45
NLANT-AN NGGUNGKONGKASIS-ANGGUNGKONGKO NGKONGKONGKONGKIS-111	1975-2050000000005-153.0000000000029406.00000000000000055005

Figure5: Combined Hash Values Of One & Two Block- Message

an Turba C++ BE	- D x
ana pana pana pana pana pana pana pana	and and and
we-black weicome:	
ILANE-32 Norma Second Full Domail (23) 2000 IS 15 Across 22 Commun Recomments 21 Norm (26)	
ILA HE-28 Names de monores de l'onnames de 4400 milita 25 communistration de 5 communis de l'homen de 14 p	
KLAKE-64 meneralakan na pananakan na pananakan na pananakan na pananakan na na pananakan na na pananakan na pananakan na meneralah na meneralakan na pananakan na pananakan na pananakan na pananakan na pananakan na pananakan na panan	000000153
КСАХЕ—48 анализителением 10,0-респусталистически раз т. жижи сполозованиеми 15,1 постоя окончанием 74 кр. ногослени анализителе (1993) 5,155	anaoo aan
ine-black mennage:	
ILAND-12 Nobel 12 Novembry 2 2000 (1.1.2 You was not Propert 2 You was 2 1 1 1000 (2 You was called	
ILANE - 28 Norts as agreets (32,0000), 71,900,000,03,300,000,020,700,000, 46,900,000,700	
КАХЕ-44 настоящиеськиет, рас сполокомистически, с № литиковологических с 4 написаномистических №АХ потолном полоситиковании с 2 Палиболимистически а раковорскотических с 10 П.	ennemedado:
ILA K1 - 48 Internationalisti 2.47 Pointanaooninali (2.42 Pointase Dessen 73 74, duinese Donato (74). Humane D Insertationalisti (46 FA	08800-6272
two-block mennage)	
ILA KE-12 NUMY 35 LANNELYS EDEDDDD 37 20086 LYNN BORDS 22 NARRES 8 LCARREDY 3 LANNEC 36.4	
II.A KE-20 Norts Canadaes & Fooder (1744/08/06/35/08/08/03/27/08/08/5038/28/08/17/17	
ela kel-64 Herrandon on V. 71 den konstanter (* 15 van Andrea Santa, Van Herrandon en 155 (Herrando Herrandon en 11 hande de de senter (* 15 herrandon de senter (* 14)	0000000151

Figure6: Changed Combined Hash Value Of One & Two- Block Message

CONCLUSION

A cryptographic hash function is a hash function, that is, an algorithm that takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value, such that an (accidental or intentional) change to the data will (with very high probability) change the hash value. In this work the comparison of two SHA-3 cryptography hash function JH and BLAKE, less time consuming process BLAKE-256 with 14 rounds instead of 64 rounds of SHA-256, more reliable compare to SHA family. This work gives the comparative hash algorithms of both candidates.

FUTURE WORK

In future the working of the function (BLAKE-256) discussed here should be more less time consuming. It can be merge all three function of BLAKE-256 into single unit in VHDL then give one time input (256 bit) and get 256 bit final hash value.

REFERENCES

- [1] FPGA Based Area And Throughput Implementation of JH And BLAKE Hash Function http://www.ijcttjournal.org/volume-3/issue-2/IJCTT-V3I2P112.pdf
- [2] Comparative Study of Two SHA-3
 Cryptographic Hash Function JH and BLAKE
 Vaibhav Doshi ,Richa Arya,Birbal Saran. April
 21-23,2012. ICRTCTA 2012.
 Amity School of Engineering and Technology
- [3] J. P. Aumasson , L. Henzen , W. Meier, and R.C.W. Phan, "SHA-3 Proposal BLAKE", online: http://www.131002.net/blake 2010.
- [4] Wu, H., SHA-3 proposal JH, Website: http://icsd.i2r.astar.edu.sg/staff/hongjun/jh/.

- [5] National Institute of Standard and Technology (NIST):Cryptographic Hash Algorithm Competition Website: http://csrc.nist.gov/groups/ST/hash/sha-3/.
- [6] J.P. Aumasson, L. Henzen, W. Meier, R.C.W. Phan, "SHA-3 proposal BLAKE". Submission to the SHA-3 Competition, 2008.
- [7] E. Biham, O. Dunkelman, "A framework for iterative hash functions- HAIFA".Cryptology ePrint Archive, Report 2007/278.
- [8] Mao Ming,He Qiang ,Shaokun Zeng Xidian University Xi'an , Shanxi, China BLAKE- 32 based on differential properties, 2010 International Conference on Computational and Information Sciences.
- [9] George Provelengios, Nikolaos S. Voros, Paris Kitsos Greece, 2011 14th Euromicro Conference on Digital System Design
- [10] SHA-1 Standard, National Institute of Standards and Technology (NIST), Secure Hash Standard, FIPS PUB 180-1, 1995, available on line at www.itl.nist.gov/fipspubs/ fip180 1.htm
- [11] Secure Hash Standard (SHS), National Institute of Standards and Technology(NIST),FIPS P UB 180-3,2008,available online at http://csrc.nist.gov/publications/fips/fips1803/fi ps180-3_final.pdf
- [12] IEEE Annual Symposium Nicolas Sklavos
 2010,ZIP 27100,GREECE,Paris Kitsos, Computer Science Hellenic Open University,
 GREEC.
- [13] J.-L. Beuchat, E. Okamoto, and T. Yamazaki,
 "Compact implementations of BLAKE- 32 and BLAKE-64 on FPGA," in FPT, 2010, pp. 170–177.
- [14] H. Wu. SHA-3 proposal JH, version January 15, 2009. JH

International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue 6–June 2013

- [15] Bernhard Jungk and J⁻urgen Apfelbeck, Hochschule RheinMain, Wiesbaden, Germany
 2011 International Conference on Reconfigurable Computing
- [16] D. J. Bernstein. ChaCha, a variant of Salsa20.
 Available online at http://cr.yp.
 to/chacha/chacha-20080128.pdf, January 2008.
- [17] E. Biham and O. Dunkelman. A Framework for Iterative Hash Functions - HAIFA. In Second NIST Cryptographic Hash Workshop, Santa Barbara, California, USA, August 24-25, 2006, August 2006.
- [18] Cadence Design Systems. The Cadence Design Systems Website. http://www.cadence.com/.
- [19] C. D. Canni_ere, H. Sato, and D. Watanabe. Hash Function Lufia, Specification Ver.
 2.0.Available online at http://www.sdl.hitachi. co.jp/crypto/luffa/Luffa_v2_Specificati on _20090915.pdf, September 2009.
- [20] SHA-512/256 Shay Gueron 1, 2, Simon Johnson 3, Jesse Walker4 Department of Mathematics, University of Haifa, Israel Mobility Group, Intel Corporation, Israel Development Center, Haifa, Israel Intel Architecture Group, Intel Corporation, USA Security Research Lab, Intel Labs, Intel Corporation, USA
- [21] H. Namin and M. A. Hasan, Waterloo, Ontario N2L 3G1 Canada. Compression Function for Selected SHA-3 Candidates.
- [22] Iterative Differentials, Symmetries, and Message Modification in BLAKE-256 Or Dunkelman and Dmitry Khovratovich University of Haifa, Israel Weizmann University, Israel Microsoft Research Redmond, USA

[23] Hongjun Wu, "The Hash Function JH", The First SHA-3 Candidate Conference, 2009, available online at http://ehash.iaik.tugraz.at/wiki/JH