International Journal of Interdisciplinary Innovative Research &Development (IJIIRD)
ISSN: 2456-236X
Vol. **05** Issue **01** | **2020**

Power Estimation and High Through Put MD5 Design by Unfolding Transformation

Dr. T. Menaka Devi[1]and Ambika.N[2]
[1]Faculty of Adhiyamman College of Engineering (Autonomous), Hosur,
[2]Student of Adhiyamman College of Engineering (Autonomous), Hosur

ABSTRACT

The one of hash feature utility is cryptographic and we can utilize it to reap certain protection objectives in a hardware implementation. There are four styles of MD5 designs are using to gain maximum through put. By Unfolding Transformation, the pipelining cycles in MD5 design are reduced from 32 range of pipelining to 16 stages pipelining. From this stage of reduction, we can achieve high through-put while compared with existing method (from 64 stages to 32 stages). The proposed work output is designed by Verilog coding and at a same time output is simulated by using ModelSim. Unfolding transformation of high performance pipelining's are fetched to Message Digest hash feature to gain High throughput and for improving maximum frequency. Whenever, we are capable of increasing the pipeline stages, the MD5 design performance improved significantly.

Keywords: Unfolding transformation, Maximum Frequency, High through put, MD5

1. INTRODUCTION

From the architecture of turbo decoder, we can utilize the central Add Analyze Select (ACS) activity [12]. Because of the parallel processing the ACS blocks have lower number of preparing steps, so we gain low transmission energy and less multifaceted nature about 71%. The throughput of proposed work is 1.03 Mb/s, and the memory necessity of proposed work is 128.8 Kbps, the unpredictability is decreased by 4% and the force utilization is diminished by 32%. By orthogonal Frequency Division Multiplexing (OFDM), the VLSI architecture was implemented [13]. A 4-QAM (Quadrature amplitude modulation) is favored for OFDM based remote correspondence framework. The proposed work attains high data rate with less bandwidth by reading area and power consumption and the noise in architecture has overcome by the utilization of OFDM.

Hash feature is main pillar of message authentication during data transmission and always the output should be in Message (arbitrary length) and output should be always Hash value (fixed length). The outputs are returned via hash functions (output of hash function) are called MD or hash value. Hash function provides a message with changes of 1 bit in the hash value. We have several varieties of hash features that may be used to improve throughput. From the varieties of hash futures, we utilize MD5 hash function. Pipelining is demonstrated a best answer for diminishing time in any VLSI architecture. A Direct Advanced Synthesizer (DDS) have been proposed by Madheswaran. M and Menakadevi. T [14] which utilizes half and half wave pipelining and Organize Revolution Computerized PC (CORDIC) calculation for programming characterized radios. The outcomes show the improvement of execution and effectiveness by utilizing pipelining architecture. Additionally, the data path of the pipeline was designed likewise evolved in DDS for radio network [15] which shows the better performance and also better execution. To design the high speed MD5 hash function, the high throughput must to be considered. That's why the unfolding transformation and pipelining techniques are chosen for through-put growth of MD5design. Other hash-features are SHA-1, SHA-2, both secure hash functions (SHA) are size of 160- bit. RIPEMD- 128 bit (RACE integrity primitives evaluation message digest), RIPEMD- 160bit, MD (Message Digest)-128bit Family MD2, MD 4, MD5 WHIRLPOOL -512 bit. Repeatedly the utilization of hash characteristic is MD5 was developed by Rivest. And the features of hash-function are i. fixed length output and ii. compressing the hash-functions iii. generates values between 160 to 51 bits. By low power design, the power consumption will be reduced and we can enhance the performance.

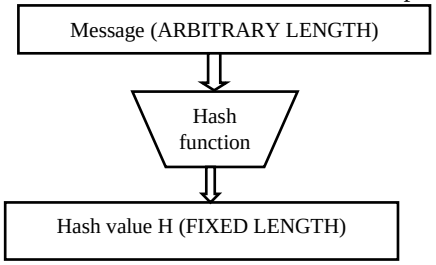


Fig. 1 Working method of Hash feature

2. THE PROPERTIES OF HASH-FUNCTION

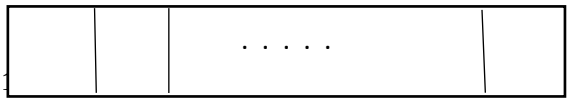
2.1. Pre- image resistance: Pre image resistance is complicated to reverse the entire process. Whenever, the hash feature(H) produces fixed length values (Z), it will likely to be tough to get the arbitrary length value (X), That matches to fixed length values.
Pre image resistance protects in opposition to an user who have only Z and attempting to get X value that matches to Z values.

2.2. Second pre- image resistance: This property says that given X and it's hash Z make tough to locate distinctive input with identical hash value (I,e.) h(Y)=h(X).
This hash function property protects against an user, who have arbitrary value and hash value but want to substitute a different value instead of duplicate value

2.3. Collision resistance (collision free hash function): Collision resistance is tough to get two different arbitrary inputs (X and Y) at any length that matches the previous hash function value. h(X)=h(Y). It is very hard for user to find 2 arbitrary values with identical hash value that matches the previous inputs

3. MD5 ALGORITHM

The message digest (MD5) algorithm is broadly usage hash function which produces one hundred- and twenty-eight-bit hash. Usually, the algorithm of message digest has two parts Namely messaging preprocessing and another one is Hash computation. In pre-processing, the design starts by padding messages in little endian format. By padded the input message with include by adding 1 bit at the fixed range of message duration. The processes in continued until the 0 bit is padded with message. In 128 bits, the sixty-four bits are resolved for period of arbitrary message. And the remaining sixty-four bits message length also in little endian format. So, the Arbitrary message total length is 512 bits. Here, after completing the message padding, the second method hash computation take place.
The total 512 bits are equally breakdown into 16 block, each block carries 32 bit.
512 bits



M [0], M[1], ……..…, M[15]

The MD5 has four Non-linear functions namely F, G, H and I .Each Non-linear functions has 16 rounds and the total rounds in a algorithm of MD5 has sixty-four to reap 128 bits of hash code. The bunch of rules in MD5has sixty-four rounds of operations. While F denotes Non-linear function, and only one characteristic is used in every round. M_i denotes a thirty-two bit of input message and K_i denotes a thirty-two bit of constant, and it's miles exceptional for each round of operation.$<<_s$ denotes left shift rotation of value s, it changes for each round of operation.$\oplus$ denote addition modulo of $2^{32.}$ The entire algorithm is divided from 128 bits into 32 bit words, and they are A, B, C and D. There are four possible functions with different Non-linear function for each round.

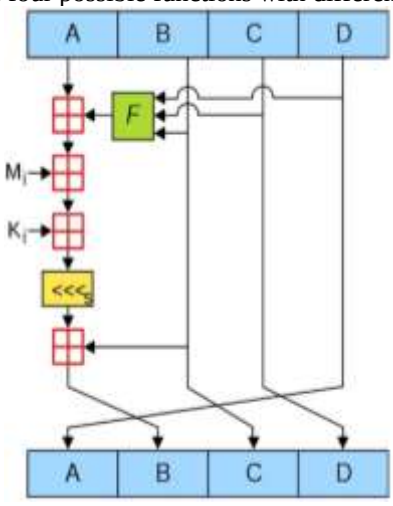


Figure: compression of MD5 algorithm

G(B,C,D)= (B ∧ D) ∨ (C ∧ ¬D)
H(B,C,D)= (B ⊕ C ⊕ D)
I(B,C,D)= (C ⊕ B ∨ ¬D)

4. PROPOSED MD5 ALGORITHM

Now a days we broadly using MD5 in message(or) data transmission with high security. MD5 is one kind of THE hash-function and we proposed the same MD5 with the unfolding transformation with 16 ranges of pipelining layout from the MD5 types mentioned above. By utilization of unfolding transformation factor of two, the huge number of varieties in pipeline cycles are reduced from 32 to 16 cycles with maximum amount of throughput and frequency using Verilog coding. We gain excessive through-put message digest (MD5) with less amount of latency via unfolding transformation.

We are using 4 iterations in proposed work instead of existing working process and can achieve better performance. This improvement in proposedMD5 design is critical for Hash-based totally Message Authentication Code (HMAC)and digital signature applications. The figure shown below illustrates the compressing characteristics of the MD5 unfolding algorithm. The below figure has four operations of MD5 which are executed in single cycle. The MD5 unfolding algorithm consists of three nonlinear functions (Func_$_t$(B,C,D) and Func_$_{t+1}$(B,C,D), four input messages (M_$_t$[k], and M_$_{t+1}$[k] and M_$_{t+2}$[k] and four constants (K_$_t$[t] and K_$_{t+1}$[t],K_$_{t+2}$[t]) and two shift values ($S_t$and$S_{t+1,}$ S_{t+2}).

The proposed MD5 algorithm has three inputs with the first nonlinear function and B and C and D. Then, the operation is commenced by means of including _$_t$[k], and a constant K[t]. The obtained result is shifted right to called as S_t. The Output T is obtained by adding another input B. Then the second Non-linear function (T, B, C) will be performed. And operation started by adding M_$_{t+1}$[k] and constantK_$_{t+1}$[t] and simultaneously the output also shifted left by the value $s_{t+1.}$ Again the output T is obtained with another Non-linear function of input M_$_{t+2}$[k] and constant K_$_{t+2}$[t] and output is left shifted by value s_{t+2}.

The functions performed in parallel wise process with different inputs and constant values. The result of restructuring the architecture of compressing the MD5into four parallel operations in a single cycle, the variety f MD5 cycles can be reduced from 32 to 16.Constant T represents the first-round output calculation of the proposed algorithm, then it miles observed by using second round which output Temp, and again followed by the third round calculation with temp.

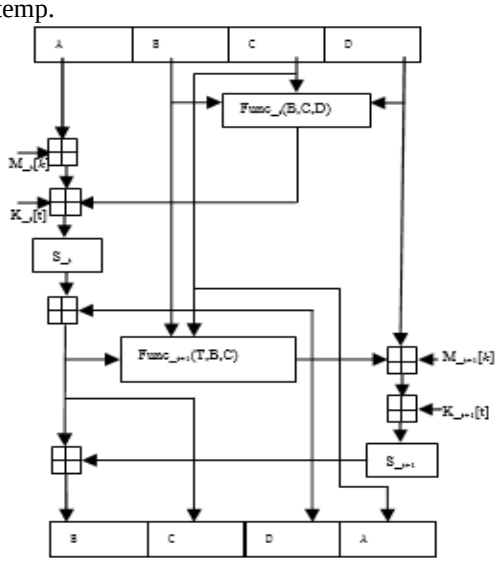


Figure: proposed compression of MD5 algorithm

4.1. TOP LEVEL UNFOLDING MD5 DESIGN

The six module names are ABCD_init, input_ABCD, MD5_initial, func_process, getdata and MD5_hash.The MD5 architecture is shown below.

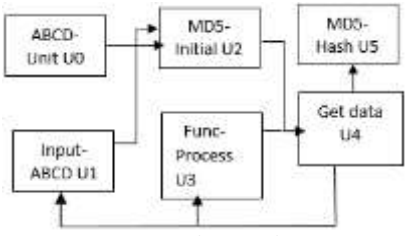


Figure: Top level unfolding of MD5 design

Top level unfolding transformation of MD5 hash-function design algorithm own 32 rounds of Non-linear functions and each unction carries 8 rounds. Top level MD5 algorithm has six modules and each module performs as their individual function.

4.2. MD5 ARCHITECTURE

The MD5 architecture is illustrated by unfolding transformation to boom the through-put of message digest (MD5) design. Based on FPGA(Field Programmable Gate Array) , four registers are requires to implement four stages of pipeline and 32 stages are required in existing method but in proposed design instead of that eight stages are required to enforce the 16 pipeline stages.
The below figure illustrate the pipelining and unfolding transformation of MD5 compression method.

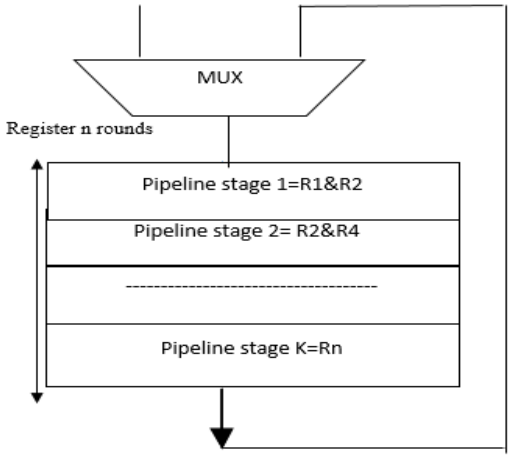


Figure: Pipelining and unfolding message digest compression function

5. RESULT AND FUTURE WORK

The unfolding transformation of MD5 design is generated from software of Model-simulation and developed by coding language of Verilog . Here we used FPGA registers to put into effect the MD5 design in an effort to gain high through-put and excessive frequency. MD5 provides high performance while we compare with other hash-functions which includes SHA and RIPEMD .The hash-function utility of MD5 provide more security in data transmission and it is using in so many real time applications example embedded security systems .And one hash utility is cryptographic, it provide tons of greater protection and it is also a one way function changes plain text to a unique digest that is irreversible
In another words, cryptographic hash-function developed to offer protection. There are 2 actual time packages of hash feature depend upon the cryptographic properties. One is Password storage and one more application is Data integrity check. The unfolding transformation of MD5 design is generated from software of Model-simulation and developed by coding language of Verilog . Here we used FPGA registers to put into effect the MD5 design in an effort to gain high through-put and excessive frequency. MD5 provides high performance while we compare with other hash-functions which includes SHA and RIPEMD .
The hash-function utility of MD5 provide more security in data transmission and it is using in so many real time applications example embedded security systems .And one hash utility is cryptographic, it provide tons of greater protection and it is also a one way function changes plain text to a unique digest that is irreversible
In another words, cryptographic hash-function developed to offer protection. There are 2 actual time packages of hash feature depend upon the cryptographic properties. One is Password storage and one more application is Data integrity check.

Figure: simulation of MD5 design

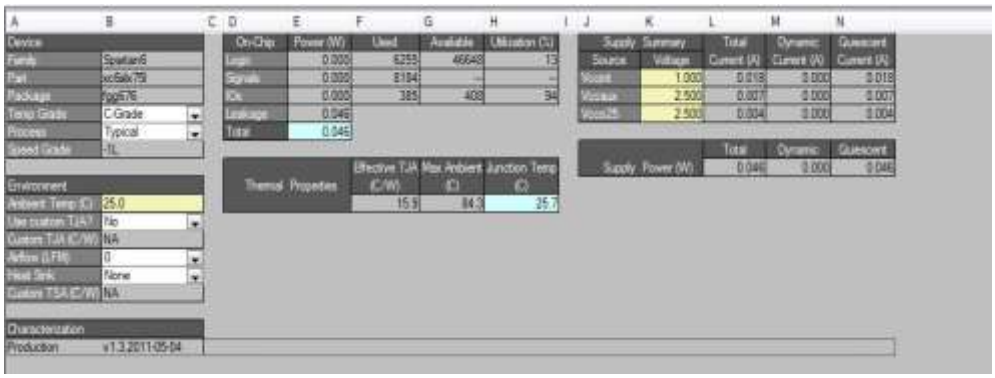


Figure: power estimation of MD5 design

The MD5 design can do the variations in area and time compared with existing algorithm. Latency will take place in the procedure of stages reduction. So, the unfolding transformation offers a high-through-put MD5 design by reducing its latency. Retiming can help us in a process of delay reduction S.

Table: I/O: Description of MD5 pipeline

INPUTS	OUTPUTS
Message (Arbitrary value) 127 bits	Digest (127.0 bits)
Clock	Value (127.0)
Reset	Valid

6. CONCLUSION

Four sorts of MD5 configuration dependent on Quartus II Arria II GX: EP2AGX45D F29C4 were effectively incorporated and actualized. The outcomes are shown that the proposed MD5 unfurling with 16 phases of pipelining gives a superior MD5 plan as far as speed, area and throughput. The output of unfolding change a throughput of MD5 to diminishing its latency. Additionally, the pipelined MD5 configuration has rapid in the increasing the frequency of pipeline. Subsequently, a MD5 configuration consolidating the unfolding change and pipelining can improve the output fundamentally. In this investigation, the maximum input arrival time before clock is 11.203ns and maximum output required time delay is 15.422ns.

7. REFERENSES

[1] F. R. Henriquez, N. A. Saqib, A. D. Perez and C. K. Koc: Cryptographic algorithms on reconfigurable hardware, Springer Series on Signals and Communication Technology, pp. 189–201, 2006.
[2] P. R. Panda, B. V. N. Silpa, A. Shrivastava and K. Gummidipudi: Chapter 2, Power-Efficient System Design, Springer Science Business Media, LLC,2010.
[3] R. L. Rivest: The MD5 message_digest algorithm, RFC 1321, MIT Laboratory for Computer Science and RSA Data Security Inc., April1992.
[4] K. K. Parhi: VLSI digital signal processing systems: Design and implementation, John Wiley & Sons Inc., pp. 119-140,1999.
[5] S. Suhaili and T. Watanabe: High throughput evaluation of SHA- 1 implementation using unfolding transformation, ARPN Journal of Engineering and Applied Sciences, ISSN 1819-6608, Vol.11, No.5, pp. 3350-3355,2016.
[6] J. Deepakumara, H. M. Heys and R. Venkatesan: FPGA implementation of MD5 hash algorithm, Proceedings of the Canadian Conference on Electrical and Computer Engineering, CCECE 2001, Toronto, Canada, Vol.2, pp. 919-924, May 13-16, 2001.
[7] J.M. Diez, S. Bojanic, L. Stanimirovic, C. Carreras and O. Nieto- Taladriz: Hash algorithms for cryptographic protocols: FPGA implementations, 10th Telecommunications forum TELFOR'2002, Belgrade Yugoslavia, Nov. 26-28,2002.
[8] K. Jarvinen, M. Tommiska and J. Skytta: Hardware imple- mentation analysis of the MD5 hash algorithm, Proceedings of the 38th Hawai International Conference on System Sciences, 2005.
[9] Y. Wang, Q. Zhao, L. Jiang and Y. Shao: Ultra high throughput implementations for MD5 hash algorithm on FPGA, High- Performance Computing and Applications, Lecture Notes in Computer Science, Vol. 5938, pp. 433-441,2010.
[10] D. He and Z. Xue: Multi-parallel architecture for MD5 implementations on FPGA with gigabit-level throughput, 2010 International Symposium on Intelligence Information Processing and Trusted Computing, pp. 535-538,2010.

[11] Menakadevi T., Madheswaran M. (2009) Design and Implementation of High Performance Viterbi Decoder for Mobile Communication Data Security. In: Herrero Á., Gastaldo P., Zunino R., Corchado E. (eds) Computational Intelligence in Security for Information Systems. Advances in Intelligent and Soft Computing, vol 63. Springer, Berlin, Heidelberg.

[12] Menakadevi. T, Anitha.V, "VLSI Architecture of a Clock-gating Turbo Encoder for Wireless Sensor Network Applications", International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 12, December 2015.

[13] T Menakadevi, R Achitha, S Bhagyalakshmi and V Jaya Sruthi, "Design and Implementation of 4–QAM VLSI Architecture for OFDM Communication", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 5, PP. 226-230.

[14] T.Madheswaran, M., Menakadevi, T. An Improved Direct Digital Synthesizer Using Hybrid Wave Pipelining and CORDIC algorithm for Software Defined Radio. *Circuits Syst Signal Process* 32, 1219–1238 (2013)

[15] T Menakadevi, M Madheswaran, "FPGA implementation of direct digital synthesizer using pipelined cordic algorithm", European Journal of Scientific Research, Vol. 79, Issue. 2, pp. 269-278.