authentication, verifying data integrity and generating digital signatures for both data origin authentication and verifying the content of the document. The hash processor proposed in this study can be used in these applications easily. The usage of the processor is flexible, since it has a serial communication interface that makes the communication with the external world possible.

References

[1] Anh Tuan Hoang, Katsuhiro Yamazaki and Shigeru Oyanagi , ,Multi-stage Pipelining MD5 Implementations on FPGA with Data Forwarding, 16th International Symposium on Field-Programmable Custom Computing Machines 2008.
[2] Changxin Li, Hongwei W, Shifeng Chen1, Xiaochao Li2 , Donghui Guo, ,Efficient Implementation for MD5-RC4 Encryption Using GPU with CUDA, 3rd International Conference on Anti-counterfeiting, Security, and Identification in Communication,. ASID 2009.
[3] Chiu-Wah Ng, Tung-Sang Ng and Kun-Wah Yip ,A UNIFIED ARCHITECTURE OF MD5 AND RIPEMD-160 HASH ALGORITHMS, ISCAS 2004
[4] Dongjing He and Zhi Xue Multi-parallel Architecture for MD5 Implementations on FPGA with Gigabit-level Throughput, International Symposium on Intelligence Information Processing and Trusted Computing, 2010**.**
[5] Feng Wang, Canqun Yang, Qiang Wu, Zhicai Shi, Constant Memory Optimizations in MD5 Crypt Cracking Algorithm on GPU-Accelerated Supercomputer Using CUDA The 7th International Conference on Computer Science & Education (ICCSE 2012). Melbourne, Australia 2012.
[6] H. Mirvaziri, Kasmiran Jumari, Mahamod Ismail, Z. Mohd Hanapi, Anew Hash Function Based on Combination of Existing Digest Algorithms , The 5th Student Conference on Research and Development – SCOReD 2007, 11-12 December 2007, Malaysia
[7] J. Touch, Report on MD5 Performance, RFC 1810, June 1995.
[8] Kimmo J, rvinen, Matti Tommiska and Jorma Skytt ,Hardware Implementation Analysis of the MD5 Hash Algorithm , Proceedings of the 38th Hawaii International Conference on System Sciences – 2005
[9] Kostas Theoharoulis, Ioannis Papaefstathiou, Charalampos Manifavas, Implementing Rainbow Tables in High-end FPGAs for Superfast Password Cracking, International Conference on Field Programmable Logic and Applications 2010.
[10] Md. Didarul Alam Chawdhury, and A.H.M. Ashfak Habib, Security Enhancement of MD5 Hashed Passwords by using the Unused Bits of TCP Header, Proceedings of 11th International Conference on Computer and Information Technology (ICCIT 2008) 25-27 December, 2008, Khulna, Bangladesh.