ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

Analysis of MD5 Algorithm Safety against Hardware Implementation of Brute Force Attack

AL-Marakeby

Systems and Computers Engineering Dept., Faculty of Engineering, Al-Azhar University, Cairo, Egypt

Abstract: MD5 is one of the most widely used hash functions generating 128 bits cipher. Theoretically, this algorithm requires 2^{128} iteration for brute force attack. This complexity represents a challenge on cracking this algorithm due to the computational time. The hardware implementation of algorithm cracking increases the speed dramatically. In addition to that, using MD5 for the encryption of weak and short passwords reduces the iterations and allow breaking the password in few seconds or minutes. In this paper, the MD5 algorithm resistivity and safety has been analysed based on FPGA implementations. Different parallel architectures for implementing the algorithm have been investigated. Different sets of strong and weak passwords have been used to test these architectures. The time for cracking the cipher has been measured indicating the performance of the MD5 algorithm.

Keywords: MD5, encryption, FPGA, password cracking

I. Introduction

In modern society, commerce activities, business, transactions and government services have been carried and offered over an open and vulnerable communications network such as Internet [11]. Identity authentication is an important method to ensure safety of these activities. Certificate based digital signature authentication and password authentication are most common at present [9]. Usually, passwords and usernames are stored in a passwords file in computer system. A hacker can attack this file to obtain all passwords or monitor the network by special tools and extract the passwords from data stream. To prevent this simple attack, passwords are not saved in plaintext, but encrypted by hashing algorithms. When user enters the password, the login subsystem re-computes the password hash and compares the hash to the hash value stored on disk to confirm password correctness [10]. MD5 is one of the most widely used hash functions in the information era although its security is suspect [8]. It compresses a piece of information with plain code and
random length into 128 bits value by hash algorithm, which is
called information distract. MD5 algorithm is irreversible and cannot recover the original plain code information from information abstraction, thus it is always believed safe[9]. However, different types of attacks can be used to break MD5 such as dictionary attack and brute force attack. Dictinary attacks uses a list of known and common passwords to break the password. Brute Force Attack is an exhaustive technique of searching password from the whole potential password space, which demands a multitude of calculation[5]. Dictionary attack is easy when the password is common while brute force attack is easy when the password is small. Brute force attack ensure breaking the scanned password space but dictionary attack may fail in many cases. Due to the computational time of brute force attack, many advanced parallel platforms are used to accelerate the processing[1][4][7]. Feng has implemented a high scalable implementation of Brute Force Attack Algorithm of MD5 Crypt on Tianhe-1A, which is the fastest heterogeneous supercomputer of the world[5]. Dongjing has used FPGA to implement Multi-parallel architecture for MD5[4]. Changxin has presented an efficient implementation for MD5-RC4 encryption using NVIDIA GPU with novel CUDA programming framework[2]. In this paper we present a parallel implementation of MD5 algorithm on FPGA. The implemented parallel cores are used to break passwords encrypted in MD5 using brute force attack. The time required to beak the passwords depends on both the hardware architecture and the length of the password. The MD5 algorithm safety and resistivity are analyzed based on the breaking times. In section 2 the MD5 algorithm is introduced. Section 3 presents the FPGA based hardware architectures used to implement the MD5 algorithm. Section 4 reports the experiments and results. Finally, section 5 gives the conclusion.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

II. MD5 ALGORITHM

MD5 is a hash algorithm introduced in 1992 by professor Ronald Rivest [6]. It is an enhanced version of its predecessor MD4. MD5 is widely used in several public key cryptographic algorithms and Internet communication in general. MD5 calculates a 128-bit digest for an arbitrary b-bit message [6].In fig.1 th etransform operation of the MD5 Algorithm is illustrated [5]. A 128-bit state which is divided into four 32-bit words is used in the main MD5 algorithm. Then the four words denoted A, B, C and D, are initialized to certain fixed constants[2]. The algorithm consists of 4 main rounds with each round applying the basic operation 16 times. There are 4 different functions for the 4 rounds given in equations (1) and (2)[6]. The index i represents each step, and Xj [k] represents one message word. The orders of the 16 words for processing are different for different rounds. In the figure, K[i] is a 32-bit constant chosen from a fixed table containing 64 constants stated in the specification [3]. Table1 gives some constants for variables T,S , and index J for the message subpart. The complete table contains 64 rows for all steps.

$$A = B + ((A + \mathrm{Func}(B,C,D) + X_j[k] + T[i]) \lll s)$$
$$A \leftarrow D, B \leftarrow A, C \leftarrow B, D \leftarrow C \qquad (1)$$

$$\begin{aligned} F(X,Y,Z) &= (X \wedge Y) \vee (\neg X \wedge Z) \\ G(X,Y,Z) &= (X \wedge Z) \vee (Y \wedge \neg Z) \\ H(X,Y,Z) &= X \oplus Y \oplus Z \\ I(X,Y,Z) &= Y \oplus (X \vee \neg Z) \end{aligned} \qquad (2)$$

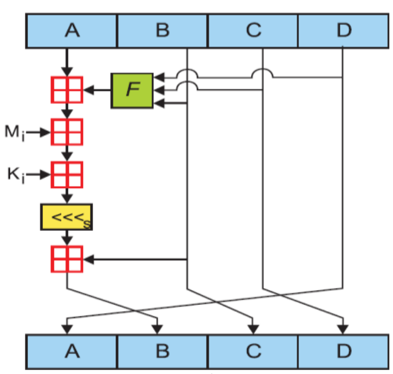

Fig.1 MD5 Transform Operation

Table.1 Samples of constants values

Step	S	T	J
0	7	0xd76aa478	0
1	12	0xe8c7b756	1
2	17	0x242070db	2

The output of the MD5 algorithm is a 128 bit cipher for all password lengths. Table2 shows samples for some passwords and the corresponding MD5 digest.

Table 2 Samples of passwords and their ciphers

Password	Cipher
Ali99	b91f419b5388b5df94804ed640914471
ashraf10	c16ffe25368eaddba046ca3ef4c71fd0
abcdef	e80b5017098950fc58aad83c8c14978e

III. FPGA HARDWARE ARCHITECTURE

FPGA (Field Programmable Gate Array) is an excellent hardware platform for implementing custom functions and parallel processing. FPGA chip contains hundreds of thousands or millions of logic elements that can be programmed to implement any function. Deploying several modules of the same function allow the parallel processing. Two different architecture are implemented to test the brute force attack for MD5.

Architecture 1: In this architecture, a straightforward implementation of parallel MD5 modules are used as illustrated in fig.2.

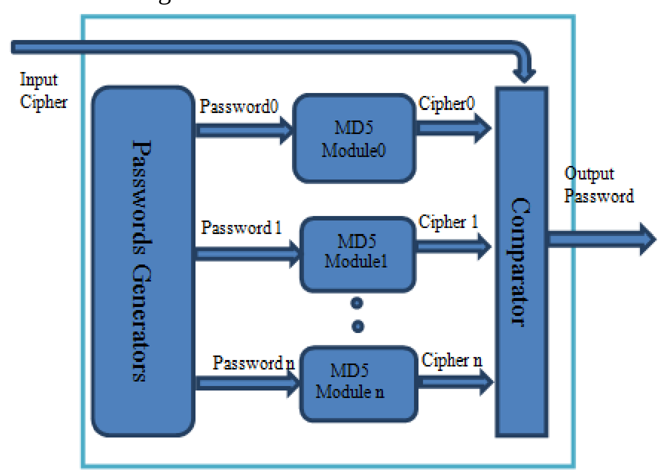

Fig. 2 Architecture 1 for brute force attack of MD5

The input of the system is the cipher and the output is the password corresponding to this cipher. Figure 2 is a simplified diagram while many details are removed or simplification. The passwords generator module consists of simple counters

which are incremented by constant values after each fail trial.

These counters are initialized by values of ASCII code of valid password characters. For each trial the right most counter are incremented by a value equal to the number of MD5 module in the system. For example if the current trial checks the password "Caira", pawword0 will be "Caira", password1 will be "Cairb" , and password9 will be "Cairj".If the number of MD5 modules is 10, the second iteration will start with the word "Cairk". The MD5 module input is the password and its output is the 128 bits cipher. The outputs of all modules are compared to the input cipher for the system. If there is no match, a new trial starts with the incremented

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

counters. A control unit is designed to send all control signals and read status of all modules in the system. There are two important parameters affects the performance of this system. The first is the number of logic elements required to implement a single MD5 module. This parameter determine the total number of MD5 modules can be fit in FPGA chip and hence affects the speed of the system. The second parameter is the clock frequency operating the system, which depends on the design of logic circuits implementing MD5 functions and steps. More details of these parameters are discussed in section 4.

Architecture 2: In this architecture a more sophisticated circuits have been designed as illustrated in fig.3. The idea of this design is to divide the single MD5 modules into two parts. The first part which is common for all modules and this include tables, some counters , registers and control circuits. The second part which is dedicated to each MD5 module and depends on the values of passwords. This part includes the logic functions of the round , internal registers A,B,C,D and other control circuits. A single module of the first part (tables and counters) is designed and shared for all modules in the system. Many modules of the second part (Round logic functions) are used to calculate the cipher for different passwords generated from password generator module. This architecture has the advantages of smaller space and hence increasing the number of modules and increasing the speed.

IV. RESULTS AND IMPLEMENTATION

Both architectures 1 and 2 discussed in section 3 are implemented on Altera DE2 FPGA board. This board contains cyclone II FPGA chip with 35,000 LEs. The Quratus II software is used to design and simulate the system. The design is written in Verilog language.

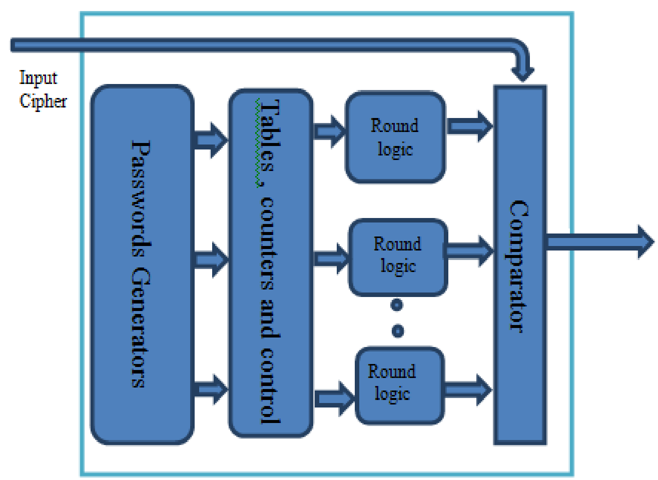

Fig. 3 Architecture 2 for brute force attack of MD5

The FPGA board has two clocks , 27 MHz and 50 MHz . Different frequency are required to our system and they are generated using frequency dividers and frequency multipliers. Simple counters are used for frequency dividers while phase locked loops are used for frequency multipliers. For Architecture 1 the FPGA chip was sufficient for only 10 MD5 modules. The clock used for this architecture is the 27 MHz divided by 8. The total performance of architecture 1 is 520K trials/sec. The second architecture works with 400 MHz clock. A PLL is used to generate this clock from the 50MHz available in the board. This clock is not the MD5 step clock, but the clock to perform micro-operations within a single step. We make analysis for the time required for each micro-operation inside the step of MD5 algorithm such as addition, increment , shift , rotation, register transfer ….etc. An optimization has been done for some operations to increase the speed. The single step requires 4 micro-operations with 16 clocks. The single trial require 64 steps.

Due to the reduced size of MD5 module in architecture 2 as discussed in section 3, 30 parallel MD5 modules are implemented on the FPGA chip. The total performance of architecture 2 is 11.7 M tirlas/sec. Table 3 gives the cracking time for different sizes passwords. Some values of this table are experimentally measured, while some other values are mathematically calculated from the architecture speed due to the very long time required to crack them experimentally.

Figure 4 shows the Altera DE2 board running the brute force attack for MD5 algorithm.

Table .4 calculated time for cracking passwords

Password	Cracking time in sec.	
	Architecture 1	Architecture 2
SFHA	13 sec	0.5 sec
Aqwe	5 sec	0.22 sec
sEwert	23,400 sec	1,041 sec
AweRTs	22,800 sec	1,014 sec
QwEsRTE	180,000 sec	8,012 sec
EdRTsWe	871,000 sec	38,000 sec
DeSSaWeP	22,500,000 sec	1,001,600 sec

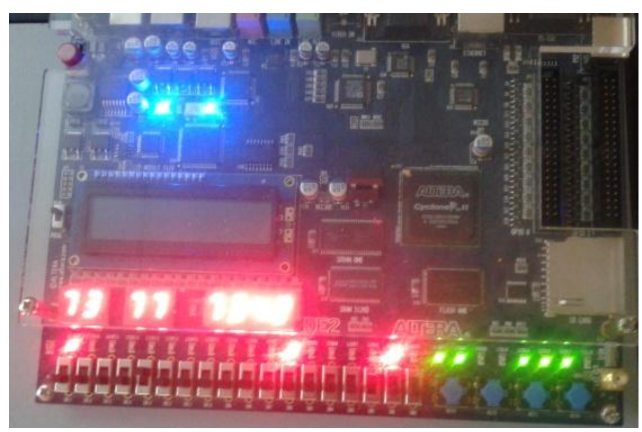

Fig.4 Altera DE2 board running brute force attack for MD5 Algorithm

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

V. CONCLUSION

Using MD5 for the encryption of passwords is not completely safe. The availability of advanced parallel processing platforms allow the breaking of this algorithm. FPGA boards, which cost hundreds of dollars, may be available to hackers and used to hack the passwords. Using short and weak passwords increase the danger of cracking the algorithm. Passwords consists of 7 characters can be cracked within 10 hours using this system. Finally using more advanced FPGA kits with faster speed and larger capacity gives better performance than given in this research and threaten the MD5 algorithm more and more.

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] 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
[7] Kostas Theoharoulis, Ioannis Papaefstathiou, Charalampos Manifavas, Implementing Rainbow Tables in High-end FPGAs for Super-fast Password Cracking, International Conference on Field Programmable Logic and Applications 2010.
[8] Ming.Mao Shaohui.Chen Yanjun.Li Shaokun.Zeng , "Construction of the skipping steps for preimage attack of MD5" Proceedings of the International Conference on Information and Automation June 20 - 23, Harbin, China, IEEE 2010
[9] Xiaoling Zheng Jidong Jin,Research for the Application and Safety of MD5 Algorithm in Password Authentication , 9th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD 2012)
[10] Yoginder S. Dandass , Using FPGAs to Parallelize Dictionary Attacks for Password Cracking, Proceedings of the 41st Hawaii International Conference on System Sciences - 2008
[11] Zhe Chen, Shize Guo, Rong Duan, Sheng Wang ,Security Analysis on Mutual Authentication against Man-in-the-Middle Attack, The 1st International Conference on Information Science and Engineering (ICISE2009)