ENHANCEMENT OF MANCHESTER ENCODING TECHNIQUE BY COMBINING IT WITH A HASH FUNCTION

A dissertation submitted to the Faculty of Information Technology

in partial fulfillment of the requirements for the degree

Master of Science (Information Technology)

Universiti Utara Malaysia

By

Mu'taz M. N. Hamarsheh

ENHANCEMENT OF MANCHESTER ENCODING TECHNIQUE BY COMBINING IT WITH A HASH FUNCTION

KOLEJ SASTERA DAN SAINS
(College of Arts and Sciences)
Universiti Utara Malaysia

PERAKUAN KERJA KERTAS PROJEK
(Certificate of Project Paper)

Saya, yang bertandatangan, memperakukan bahawa
(I, the undersigned, certify that)

MU'TAZ M.N. HAMARSHEH

calon untuk Ijazah
(candidate for the degree of) **MSc. (Information Technology)**

telah mengemukakan kertas projek yang bertajuk
(has presented his/her project paper of the following title)

ENHANCEMENT OF MANCHESTER ENCODING TECHNIQUE BY COMBINING IT WITH A HASH FUNCTION

seperti yang tercatat di muka surat tajuk dan kulit kertas projek
(as it appears on the title page and front cover of project paper)

bahawa kertas projek tersebut boleh diterima dari segi bentuk serta kandungan dan meliputi bidang ilmu dengan memuaskan.
(that the project paper acceptable in form and content, and that a satisfactory knowledge of the field is covered by the project paper).

Nama Penyelia Utama
(Name of Main Supervisor): **DR. NOR LAILY HASHIM**

Tandatangan
(Signature) : _____

DR. NOR LAILY HASHIM
Head Coordinator
Graduate Department of Information Technology
College Arts & Sciences
Universiti Utara Malaysia

Tarikh
(Date) : 20/5/2008

PERMISSION TO USE

In presenting this thesis in partial fulfillment of the requirements for a postgraduate degree from Universiti Utara Malaysia, I agree that the University Library may make it freely available for inspection. I further agree that permission for copying of this thesis in any manner, in whole or in part, for scholarly purpose may be granted by my supervisor(s) or, in their absence by the Dean of Faculty of Information Technology. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Request for permission to copy or to make use of material in thesis in whole or in part should be addressed to:

Dean of Faculty of Information Technology
Universiti Utara Malaysia
06010 UUM Sintok
Kedah Darul Aman

DEDICATION

In loving memory of my late father,

My great beloved mum,

My supportive and caring brothers,

My beloved kind sisters,

My sweetie nephews and nieces

My work is dedicated to all of you my heart residents

ABSTRACT

This study proposes a combination of Manchester encoding technique and SHA-1 hash function, to provide a secure data transmission over a client/server environment by sending the message digest along with the message, and compare it with a new generated message digest on the server. Hash function improves integrity to the transmitted message. Manchester encoding technique is chosen to encode the transmitted message because it encodes both data and clocks into a form of synchronous bit stream. The modification of the message during the transmission, results in changing the message digest. This shows that including the SHA-1 hash function with Manchester encoding technique the integrity of the data can be accomplished.

ACKNOWLEDGMENT

بسم الله الرحمن الرحيم

I am grateful for all those who contributed to this study. I am particularly grateful to my supervisor Dr. Nor Laily Hashim who has been my true support from the beginning to the end of this project. My thanks also to my family and my friends for their feelings and support.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

MET	Manchester Encoding Technique
SHA-1	Secure Hash Algorithm 1
DC	Direct Current, *Continuous* Current
MAC	Message Authentication Code
HMAC	Keyed-Hash Message Authentication Code
DTE	Data Terminal Equipment
EBCDIC	Extended Binary Coded Decimal Interchange Code
ASCII	American Standard Committee for Information Interchange
DPLL	Digital Phase Locked Loop
DSS	Digital Signature Standard
NIST	National Institute of Standards and technology
DSA	Digital Signature Algorithm
FIPS	Federal Information Processing Standards

CHAPTER ONE

INTRODUCTION

1.1 Preamble

With the introduction of the computer and the advent of computer networks, the need for protecting information becomes more important. The transmitted data through the open networks may fall into wrong hands or get altered without the knowledge of senders or receivers of the message (Dahlin & Krantz, 2001).

In recent years, automated tools were required for protecting sensitive data from flowing over these networks. Cryptography came as a clear answer to all these concerns.

Large amounts and various types of data are transferred through hundred of networks daily. This data is subjected to hacking during its transmission through networks as shown in Figure 1.1. An example is the client/server system where client sends data to the server and vice versa (Stallings, 2006b).

The contents of the thesis is for internal user only

References

Alho, T., Hämäläinen, P., Hännikäinen, M., and Hämäläinen, T. D. (2007). Compact Hardware Design of Whirlpool Hashing Core. In *Proceedings of the Conference on Design, Automation and Test in Europe* (Nice, France, April 16 - 20, 2007). Design, Automation, and Test in Europe. EDA Consortium, San Jose, CA, 1247-1252. ACM.

A Look At Signal Encoding, Retrieved in January 26, 2008 at 9:40 pm. From: http://www.commsplace.com/Knowledge/ITcs/html/tutorials/encoding/gigabit.htm

A Sun Developer Network Site (2008), What Is a Socket? (The Java™ Tutorials > Custom Networking > All about Sockets). Retrieved in April 15, 2008 at 7:55 am. From: http://java.sun.com/docs/books/tutorial/networking/sockets/definition.html

Barreto P (2006), The WHIRLPOOL Hash Function. Retrieved in March 2, 2008 at 3:00 pm. From: http://paginas.terra.com.br/informatica/paulobarreto/WhirlpoolPage.html

Bertoni, G., Daemen, J., Assche, G. V., & Peeters, M. (2006). Radiogatun, A Belt-And-Mill Hash Function. *Second Hash Workshop of NIST*. Retrieved: February 5, 2008. From: http://csrc.nist.gov/pki/HashWorkshop/2006/Papers/VANASSCHE_Radio Gatun_0720.pdf

Boer, B. d., & Bosselaers, A. (1994). Collisions for the Compression Function of MD5. *Advances in Cryptology--Eurocrypt, 93*. Retrieved: January 10, 2008. From: http://homes.esat.kuleuven.be/~cosicart/pdf/AB-9300.pdf

Chia-Hung, L. U., Hao-Kuan, T. S. O., & Der-Chyuan, L. O. U. (2007). Image Authentication Method by Combining Digital Signature and Watermarking. *International Journal of Computer Sciences and Engineering Systems, 1, No. 2,* 77 - 83. Retrieved: March 15, 2008. From: http://bit.kuas.edu.tw/~ijcses/v1/n2/v1-2-2.pdf

Dahlin, T., & Krantz, D. (2001). Wireless Data Link. *Circuit Cellar*, 10-19. Retrieved: January 9, 2008. From: http://www.circuitcellar.com/library/print/0601/dahlin131/dahlin131.pdf

Debaert, C. and Gilbert, H. 2002. The RIPEMD and RIPEMD Improved Variants of MD4 Are Not Collision Free. In *Revised Papers From the 8th international Workshop on Fast Software Encryption* (April 02 - 04, 2001). M. Matsui, Ed. Lecture Notes in Computer Science, *vol. 2355*, 52-65. Springer - Verlag, London.

Eastlake, D., & Jones, P. (2001). *US Secure Hash Algorithm 1 (SHA1)*: Network Working Group. Retrieved: April 20, 2008. From: http://www.ietf.org/rfc/rfc3174.txt

ECRYPT, N. E. (2004). Recent Collision Attacks on Hash Functions: ECRYPT Position Paper: ECRYPT Document STVL-ERICS-2-HASH STMT-1.0, Nov. Retrieved: April 1, 2008. From: http://www.ecrypt.eu.org/documents/ECRYPT-hash-statement.pdf

Fairhurst G (2007), Manchester Encoding. Retrieved in January 2, 2008 at 4:50pm. From: http://www.erg.abdn.ac.uk/users/gorry/course/phy-pages/man.html

FIPS, P. U. B. (2000). 186-2, Digital Signature Standard (DSS). *US Department of Commerce/National Institute of Standards and Technology*. Retrieved: April 5, 2008. From: http://www.itl.nist.gov/fipspubs/fip186.htm

Forouzan, B. A., & Fegan, S. C. (2004). *Data Communications and Networking* (3rd ed.): McGraw-Hill.

Forster, R. (2000). Manchester Encoding: Opposing Definitions Resolved. *Engineering Science and Education Journal, 9*(6), 278-280. IEEE.

Goldstein, S. C., & Rosewater, D. (2002). Digital Logic Using Molecular Electronics. *Solid-State Circuits Conference, 2002. Digest of Technical Papers. ISSCC. 2002 IEEE International, 1*, 204-459. IEEE.

Halsall, F. (1996). *Data Communications, Computer Networks and Open Systems* (4th ed.): Addison Wesley Longman Publishing Co., Inc. Redwood City, CA, USA.

Hura, G. S., & Singhal, M. (2001). *Data and Computer Communications: Networking and Internetworking* (4th ed.): CRC Press.

Jäppilä, P., & Pöyhönen, P. The Internet Security. Retrieved: February 25, 2008. From: http://keskus.hut.fi/opetus/s38130/s98/security/secfinal.pdf

Jimenez, J., Martin, J. L., Astarloa, A., & Zuloaga, A. (2004). Manchester Decoding Algorithm for Multifunction Vehicle Bus. *IEEE International Conference on Industrial Technology (ICIT), 2*, 769- 774. IEEE.

Johnson, T., Sobot, R., & Stapleton, S. (2007). Manchester Encoded Bandpass Sigma-Delta Modulation For RF Class D Amplifiers. *Circuits, Devices & Systems, IET, 1*(1), 21-26. IEEE.

Kang, Y. k., Kim, D. W., Kown, T. W., & Choi, J. R. (2002). An Efficient Implementation of Hash Function Processor for IPSEC. *Proceedings 2002 IEEE Asia-Pacific Conference on ASIC,* August *2002*, 93-96. IEEE.

Karras, D., & Zorkadis, V. (2000). A Novel Suite of Tests for Evaluating One-Way Hash Functions for Electronic Commerce Applications. *Proceedings of The 26th EUROMICRO Conference, 2*, 464 - 468. IEEE.

Karvonen, H., Shelby, Z., & Pomalaza-Raez, C. (2004). Coding for energy efficient wireless embedded networks. *International Workshop on Wireless Ad-Hoc Networks (IWWAN)*, 300–304. IEEE.

Kim, J., Biryukov, A., Preneel, B., & Hong, S. (2006). On the Security of HMAC and NMAC Based on HAVAL, MD4, MD5, SHA-0 and SHA-1. *Security and cryptography for networks, proceedings, 4116*, 242–256. Springer-verlag berlin

Kitsos, P., & Koufopavlou, O. (2004). Whirlpool Hash Function: Architecture and VLSI Implementation. *IEEE International Symposium on Circuits & Systems (ISCAS'04), 2*, 893 - 896. IEEE.

MacEwen, N. C., Crockett, l. H., Pfann, E., & Stewart, R. W. (2005). Symbol Synchronisation Implementation for Low-Power RF Communication in Wireless Sensor Networks. *Institute of Electrical and Electronics Engineers, Inc*, 447 - 451.

Merwe, P. B. v. d. (2004). *Mobile Commerce Over Gsm: A Banking Perspective On Security* University of Pretoria. Retrieved: April 12, 2008. From: http://upetd.up.ac.za/thesis/available/etd-07202004-111814/unrestricted/00dissertation .pdf

Mills, A. (2005). Manchester encoding using RS232. Retrieved: March 11, 2008. From: http://fatiherdem.net/dosyalar/Manchester_encoding_using_RS232.pdf

Polk, W., Housley, R., & Bassham, L. (2002). *Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.* Retrieved: January 15, 2008. From: http://www.faqs.org/rfcs/rfc3279.html

Popescu, P., Solheim, A., & Wight, M. (1995). Experimental monolithic high speed transceiver for Manchesterencoded data. *Proceedings of the 1995 Bipolar/BiCMOS Circuits and Technology Meeting*, 110-113. IEEE.

Ragab, A. H. M., Ismail, N. A., & Allah, O. S. F. (2001). An efficient message digest algorithm (MD) for data security. *Proceedings of IEEE Region 10 International Conference on Electrical and Electronic Technology, 2001. TENCON. 1*, 191 - 197. IEEE.

Reynders, D., & Wright, E. (2003). *Practical TCP/IP and Ethernet Networking.* Burlington: Elsevier.

Rivest, R. (1992a). *The MD4 Message-Digest Algorithm*: Network Working Group. Retrieved: March 27, 2008. From: http://tools.ietf.org/html/rfc1320

Rivest, R. (1992b). *The MD5 Message Digest Algorithm*: Network Working Group. Retrieved: March 25, 2008. From: http://tools.ietf.org/html/rfc1321

Schaad, J., Kaliski, B., & Housley, R. (2005). *Additional Algorithms and Identifiers for RSA Cryptography for Use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*: Network Working Group. Retrieved: March 23, 2008. From: http://www.ietf.org/rfc/rfc4055.txt

Schmidt, R. N., Buckett, J. R., & Hendrix, S. P. (1998). Wireless EEG System for Effective Auditory Evoked Response. *Assignee Cleveland Medical Devices Inc.*

Schmieg S (2006), How to build your own wireless receiver and transmitter device? Use RF in your next embedded application design!. Retrieved in January 7, 2008 at 8:20 pm. From: http://www.e-dsp.com/how-to-build-your-own-wireless-receiver-and-transmitter-device-create-rf-in-your-embedded-application/

Simonds, F. (1995). Network security: data and voice communications: McGraw-Hill, Inc. Hightstown, NJ, USA.

Stallings, W. (2006a). Cryptography and Network Security: Principles and Practices (4th ed.): Prentice Hall.

Stallings, W. (2006b). *Data and Computer Communications*: Prentice Hall.

Toma, D., Perez, A., Borrione, D., & Bergeret, E. (2004). Design of a Proven Correct SHA Circuit. *2004 International Conference on Electrical, Electronic and Computer Engineering, 2004. ICEEC'04.* 31-34. IEEE.

Tung, S., & Jones, A. K. (2007). An Architectural Approach for Reducing Power and Increasing Security of RFID Tags. Retrieved: January 12, 2008. From: http://www.sigda.org/daforum/accepted_2007/submission_34.pdf

Vaishnavi V & Kuechler B (2007), Design research in Information Systems. Retrieved in April 9, 2008 at 05:20pm. From: http://www.isworld.org/Researchdesign/drisISworld.htm

Wang, X., Feng, D., Lai, X., & Yu, H. (2004). Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD. C*ryptology ePrint Archive: Report 2004/199*, *Short talk presented at CRYPTO.* 1-18. Retrieved: April 13, 2008. From: http://eprint.iacr.org/2004/199.pdf

Wang, X., Lai, X., Feng, D., Chen, H., & Yu, X. (2005). Cryptanalysis of the Hash Functions MD4 and RIPEMD. *Advances in Cryptology–Eurocrypt 2005, Lecture Notes in Computer Science, 3494.* 1–18. Retrieved: February 18, 2008. From: http://www.quequero.org/uicwiki/images/Cryptanalysis_of_MD4_and_RIPEMD.pdf

Wen, C.-Y., & Yang, K.-T. (2006). Image Authentication for Digital Image Evidence. *Forensic Science Journal, 5, No. 1.* 1 – 11. Retrieved: March 22, 2008. From: http://www.cpu.edu.tw/~fsjournal/content/vol5.no.1/01(p1-p11).pdf

Xiaoning, X., Haibin, Y., & Shuping, C. (2007). A Low-Power Protocol Processor Based on NAND-Type TCAMs for Networked Sensors. *International Conference on Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007.* 2572-2575. IEEE.

Yalçin, M. E., & Vandewalle, O. (2002). Fragile Watermarking and Unkeyed Hash Function Implementation for Image Authentication on CNN-UM. *Proceedings of the 2002 7th IEEE International Workshop on Cellular Neural Networks and Their Applications, 2002. (CNNA 2002).* 399 - 406. IEEE.

Yee, L. P., & Silva, L. C. D. (2002). Application of Multilayer Perceptron Network as a One-Way Hash Function. *Proceedings of the 2002 International Joint Conference on Neural Networks, 2002. IJCNN'02., 2,* 1459 - 1462. IEEE.

Yi, X. (2005). Hash Function Based on Chaotic Tent Maps. *Circuits and Systems II: Express Briefs, IEEE Transactions on [see also Circuits and Systems II: Analog and Digital Signal Processing, IEEE Transactions on], 52(6),* 354-357. IEEE.

Yusoff, H. B. H., Bakar, A. Z. A., & Alias, R. A. (2006). Polygraphic Counterproductive Behavior Index Profiling System. *Proceedings of the Postgraduate Annual Research Seminar 2006,* 308 - 313. Retrieved: January 4, 2008. From: http://eprints.utm.my/3349/1/POLYGRAPHIC_COUNTERPRODUCTIVE.pdf

Zhang, J., Chi, N., Holm-Nielsen, P. V., Peurheret, C., & Jeppesen, P. (2004). Method for high-speed Manchester encoded optical signal generation. *Technical Digest Optical Fiber Communication Conference, 2004, USA. OFC 2004, 1.* IEEE.

Zheng, Y., Pieprzyk, J., and Seberry, J. 1993. HAVAL - A One-Way Hashing Algorithm with Variable Length of Output. In *Proceedings of the Workshop on the theory and Application of Cryptographic Techniques: Advances in Cryptology (December 13 - 16, 1992). 718.* Springer-Verlag, London, 83-104.

Zuniga, M., & Krishnamachari, B. (2004). Analyzing the transitional region in low power wireless links. *First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004.* 517-526. IEEE.