An Improved Linear Feedback Shift Register (LFSR- based) Stream Cipher Generator

A thesis submitted to the Graduate School in partial fulfillment of the requirements for the degree Master of Science (Information Technology)
Universiti Utara Malaysia

By

Reyadh H. mahdi (89037)

PERMISSION TO USE

In presenting this thesis in partial fulfillment of the requirements for a postgraduate degree from University 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 purposes may be granted by my supervisor in his absence, by the Dean of the Faculty of Information Technology. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain should not be allowed without my written permission. It is also understood that due recognition shall be given to me and to University Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Requests for permission to copy or to make other use of materials in this 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

Abstract

Linear feedback shift register (LFSR-based) stream cipher an improved design for a random key generator in a stream cipher algorithm. The proposed random key generator is simply designed to produce a very quick algorithm to be used for securing GSM communication as mobiles or in satellite communications channels, and it use to avoid attack that happen on cryptography in general and on stream cipher in specific. The simplicity of the design derived from using of four small LFSR and three Xored gates and a single (3 to 1) multiplexer on the content of 8-stages LFSR.

ACKNOWLEDGEMENTS

I would like to offer my sincere thanks to my supervisor Associate Professor Hatim Mohamad Tahir, for his excellent guidance and moral support, his time and for his patience and commitment in helping me complete this research.

I would also like to offer my deepest gratitude to my family, for helping me, and for encouraging me to do my master, which enabled me to successfully accomplish my tasks.

I am deeply indebted to my dear friends and staff in UUM especially from the Faculty of Information Technology for taking so much of interest in my work, always being there for me through my difficult situations and spending their time in guiding me despite their busy schedule.

Last but not least, thanks to all those who have been directly and indirectly involved in helping me completing this research.

CONTENT

LIST OF FIGURE

LIST OF ABBREVIATIONS

LFSR	Linear Feedback Sift Register
RSA	Rivest, Shamir, and Adleman
DES	Data Encryption Standard
HMAC	Hash Message Authentication Code
FIPC	Federal Information Processing Standards
SHA	Secure Hash Algorithm
AES	Advanced Encryption Standard
TDES	Triple DES
NIST	National Institute of Standards and Technology
MACs	Message Authentication Codes
CBC-MAC	Cipher Block Chaining-Message Authentication Code
DSA	Digital Signature Algorithms
ECDSA	Elliptic Curve Digital Signature Algorithm
RNGs	Random Number Generation
PRNG	Pseudorandom Random Number Generation
XOR	Eexclusive-Or
SSL	Secure Sockets Layer
ASCII	American Standard Code of Information Interchange
SDLC	System Development Life Cycle
CTAK	Cipher Text Auto key

CHAPTER 1

INTRODUCTION

This chapter briefly explains the background of this study that mainly involves the cryptosystems in general and linear feedback shift register Based Stream Cipher Generator in specific. The majority of this chapter includes overview, problem statements, research questions, objectives of study, scope of study, and significance of research.

1.1 Overview

Cryptosystems are divided between those that are secret-key or symmetric, and those that are public-key or asymmetric. With the latter, the sender uses publicly known information to send a message to the receiver. The receiver then uses secret information to recover the message. In secret-key cryptography, the sender and receiver have previously agreed on some private information that they use for both encryption and decryption. This information must be kept secret from potential eavesdroppers.

The contents of the thesis is for internal user only

REFERENCES

[1] G.J. Simmons, editor. Contemporary Cryptology, The Science of Information Integrity. IEEE, New York, 1992.

[2] National Institute of Standards and Technology (NIST). FIPS Publication 46-2: Data Encryption Standard. December 30, 1993.

[3] E. Biham and A. Shamir. Differential Cryptanalysis of the Data Encryption Standard. Springer-Verlag, New York, 1993.

[4] M. Matsui. Linear cryptanalysis method for DES cipher. In T. Helleseth, editor, Advances in Cryptology | Eurocrypt '93, pages 386-397, Springer-Verlag, Berlin, 1994.

[5] Wikipedia, the free encyclopedia, Stream Cipher, last updated July 2008.

[6] William Stallings, "Cryptography and Network Security Principles and Practices, Fourth Edition", Prentice Hall, 2005.

[7] Schneier, B.,"Applied Cryptography", New York: Wiley, 1996.

[8] Ballardie, A., 'Core Based Trees (CBT) Multicast Routing Architecture', RFC 2201, September 1997.

[9] Bellovin, S., 'Firewall-Friendly FTP', RFC 1579, February 1994.

[10] Bellovin, S., and W. Cheswick, 'Network Firewalls', IEEE Communications Magazine, September 1994.

[11] Berners-Lee, T., and D. Connolly, 'Hypertext Markup Language – 2.0', RFC 1866, November 1995.

[12] Berners-Lee, T., R. Fielding and H. Nielsen, 'Hypertext Transfer Protocol – HTTP/1.0', RFC 1945, May 1996.

[13] Blakley, B., 'Architecture for Public-Key Infrastructure', Internet Draft, November 1996.

[14] Boeyen, S., R. Housley, T. Howes, M. Myers and P. Richard, 'Internet Public Key Infrastructure Part 2: Operational Protocols', Internet Draft, March 1997.

[15] Borenstein, N., and N. Freed, 'MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies', RFC 1521, September 1993.

[16] Borman, D., 'TELNET Authentication: Kerberos Version 4', RFC 1411, January 1993.

[17] Borman, D., 'TELNET Authentication Option', RFC 1416, February 1993.

[18] Borman, D., and C. Hedrick, 'TELNET Remote Flow Control Option', RFC 1372, October 1992.

[19] Borman, D., R. Braden and V. Jacobson, 'TCP Extensions for High Performance', RFC 1323, May 1992.

[20] A. Abdelhameed and S.A. Ibrahim. VLSI Design and Implemantation of ASICs for the Security Core of BluetoothWirelees Communication System Standard. Masters thesis. Ain Shames University. 2000-2001.

[21] S. Aissi, C. Gehrmann and K. Nyberg. Proposal for Enhancing Bluetooth Security Using an Improved Pairing Mechanism. 2004.

[22] N. Anand. An Overview of Bluetooth Security. February 2001.

[23] R. Anderson. Searching for the Optimum Correlation Attack. 1994.

[24] F. Armknecht. A linearisation attack on the Bluetooth key stream generator. 2002.

[25] . An Algebraic attack on the Bluetooth Key Stream Generator. 2004.

[26] . Algebraic Attacks on Stream Ciphers. 2004.

[27] . On Fast Algebraic Attacks. March 2004. Talk at the 9th Estonian Winter School in Computer Science, Palmse, Estonia.

[28] . On the Existence of low-degree Equations for Algebraic Attacks. 2004.

[29] F. Armknecht, J. Lano and B. Preneel. Extending the Resynchronization Attack. 2004.

[30] F. Armknecht. Algebraic Attacks and Annihilators. 2005.

[31] F. Armknecht and W. Meier. Fault attacks on Cominers with Memory. 2005. U.S.Patent No. 4,797,922.

[32] Electronics Industries Association. EIA Standard RS-232-C Interface Between Data Terminal Equipment and Data Communication Equipment Employing Serial Data Interchange. August 1969. reprinted in Telebyte Technology "Data Communication Library", Greenlawn NY, 1985.

[33] H. Bar-El. Introduction to Side Channel Attacks. 2003.

[34] A. Biryukov, C. De Cannière and G. Dellkrantz. Cryptanalysis of Safer++. 2003.

[35] A. Biryukov. Block Ciphers and Stream Ciphers: the State of the Art. 2004.

[36] G. Blewitt. Basics of the GPS Technique: Observation Equations. 1997.

[37] G. Brassard. Modern Cryptology. Springer-Verlag. 1988.

[38] C. Candolin. Security Issues for Wearable Computing and Bluetooth technology. 2000.

[39] C. De Cannière, T. Johansson and B. Preneel. Cryptanalysis of the Bluetooth Stream Cipher. 2001.

[40] V.V. Chepyzhov, T. Johansson and B. Smeets. A simple algorithm for fast correlation attacks on stream ciphers. 2003.

[41] D.E. Comer. Internetworking with TCP/IP: principles, protocols, and architecture. Prentice Hall. Englewood Cliffs, N.J.. 1988.

[42] D. Coppersmith and S. Winograd. Matrix Multiplication via Arithmetic

Progressions.1990. pp. 251–280.

[43] D. Coppersmith, H. Krawczyz and Y. Mansour. The shrinking generator. dvances in Cryptology - Crypto ’93. 1994. pp. 22–38.

[44] T.H. Cormen, C.E. Leiserson and R.L. Rivest. Introduction to Algorithms. 1990.

[45] N.T. Courtois, A. Klimov, J. Patarin and A. Shamir. An Algebraic attack on the Bluetooth Key Stream Generator. 2000. pp. 392–407.

[46] N.T. Courtois. Higher Order Correlation Attacks, XL algorithm, and Cryptanalysis of Toyocrypt. 2002.

[47] . Fast Algebraic Attacks on Stream Ciphers with Linear Feedback. 2003.pp. 177–194.

[48] N.T. Courtois and W. Meier. Algebraic Attacks on Stream Ciphers with Linear Feedback. 2003.

[49] N.T. Courtois. Algebraic Attacks on Combiners with Memory and Several Outputs. 2004.

[50] T. Cover and J.A. Thomas. Elements of Information Theory. Wiley. 1991.

[51] J. Daemen. Cipher and Hash Function Design. Ph.D. thesis. Katholieke Universiteit Leuven. 1995.

[52] A. Dasgupta. Analysis of Different types of Attacks on Stream Ciphers and Evaluationof Security of Stream Ciphers. 2005.

[53] Horner , K. Methodology as a Productivity Tool, in software Productivity, Handbook, J. Keyes (ed), New York, NY: Wind crest/McGraw-Hill, PP.97-117, 1993.

[54] Yourdon, E. A Natural Productivity in Object-Orientation, in software Productivity Handbook, J. Keyes (ed), New York, NY: Wind crest/Hill, PP.97-117, 1993.