International Journal of Computer and Internet Security.
ISSN 0974-2247 Volume 9, Number 1 (2017), pp. 13-20

http://www.irphouse.com

Algorithm Hopping Symmetric Cryptography

Dr. Mohamed Raseen
Independent Consultant,

Dr. Moh'd Radaideh
Software Engineering Department,
Amman Arab University, Amman, Jordan.

Abstract

A novel symmetric cryptography technique based on algorithm hopping is proposed in this paper. Traditional cryptography algorithms use a single encryption algorithm to encrypt the entire plain test. The proposed cryptographic system applies different encryption algorithm to encrypt different parts of plaintext. The strength of this cryptography is in hiding the internal parameters of the Cryptography. The parameters hidden are the actual encrypting algorithm that will be used to encrypt the next part of plain text, and the size of the next part that will be encrypted. The method used to determine the hidden parameters uses a pseudorandom number. This pseudorandom selection of the next encrypting algorithm is similar to the technique of Frequency Hopping Spread Spectrum which selects the next hopping frequency pseudo-randomly. This pseudorandom number is pre agreed sequence which functions as the private key in the context of cryptography. The proposed method can be applied to several of encryption algorithms. To evaluate the proposed system, a pool of non-exhaustive Boolean functions is chosen as encryption algorithm. In this case, the pseudorandom number determines the next Boolean function that will encrypt the next part of the plain text, and the second parameter. One of the primary advantages of choosing Boolean functions is that, it can be implemented using Binary Decision Diagrams (in software) and Field Programmable Gate Arrays or Application Specific Integrated Circuits (in hardware). Since these Boolean functions are implemented using logic gates, the encryption and decryption

speed will be much high compared to traditional encryption algorithms that use intense decimal number system calculations. In future, this algorithm hopping cryptography can also be extended as asymmetric cryptography to support public keys.

Keywords: Binary Decision Diagrams, Field Programmable Gate Arrays, Frequency Hopping, Symmetric Cryptography

I. INTRODUCTION

Cryptography is the process of transforming the data (plain text) into cipher text (encrypted text) using several available encryption standards and performing the vice versa in the receiver [1]. There are several well established encryption techniques. Famous among them are the symmetric key encryption techniques [1, 2].

The frequency hopping spread spectrum technique is used to provide secure mobile communication system by pseudo-randomly selecting the next frequency in which the wireless communication will occur [3, 4]. This pseudorandom sequence is agreed between the sender and receiver before the start of the communication [3, 4].

Binary decision diagrams (BDD) are pictorial representation of Boolean functions [5]. BDD is a binary tree data structure to represent Boolean functions [5]. Out of several packages available to implement BDD, one of famous is Colorado University Decision Diagram (CUDD) [6] which uses C interface. BDDs properties have been analyzed and there are several techniques to optimize the performance BDDs [7, 8, 9, 10, 11].

BDDs can be realized using Field Programmable Gate Array (FPGA) or Complex Programming Logic Devices (CPLD). C language can be used to transform the BDD to FPGA circuit [12].

The symmetric encryption can be implemented in software (JavaScript) [13] and in hardware (Application Specific Integrated Circuit – ASIC) [14]. There are concrete techniques [15] to evaluate the performance of symmetric encryption.

This paper proposes a symmetric encryption scheme that applies the concept of frequency hopping, to hop among the encryption techniques that encrypt different parts of the plain text. Section two of the paper describes the proposed system. Section three chooses Boolean function as encryption algorithms (As an example) and explains how the proposed system can be developed using the chosen Boolean function. Section four of the paper provides information about implementation details of the proposed system in Hardware and Software. Section five is about the advantages, applications and future work. Finally conclusion section concludes the paper.

II. PROPOSED SYSTEM – ALGORITHM HOPPING

Fig. 1 illustrates proposed algorithm hopping technique. Initially a pseudorandom number sequence (Private Key) is decided between the sender and receiver. This pseudorandom number sequence (24, 87, 54, 19, 72…) is shown in the left side of Fig. 1. The plain text is in the top of Fig.1. The method assumes that there are 20 encryption algorithms in the pool. Initially 24 (first number in sequence) bits of the plain text are taken and are encrypted using algorithm 7 (87 MOD 20), where 87 is the second number in sequence and 20 is the number of algorithms in the pool. This procedure is repeated for next 54 (third number in sequence) using algorithm 19 (which is 19 [fourth number in sequence] MOD 20). The encrypted chunks of data are combined together to form the cipher text shown in the bottom of Fig. 1. The algorithm used to encrypt the chunks of data are hopping pseudo-random, hence the name algorithm hopping. The decryption process in the receiver uses the same pseudo number sequence to decrypt the cipher text using the corresponding decryption algorithm.

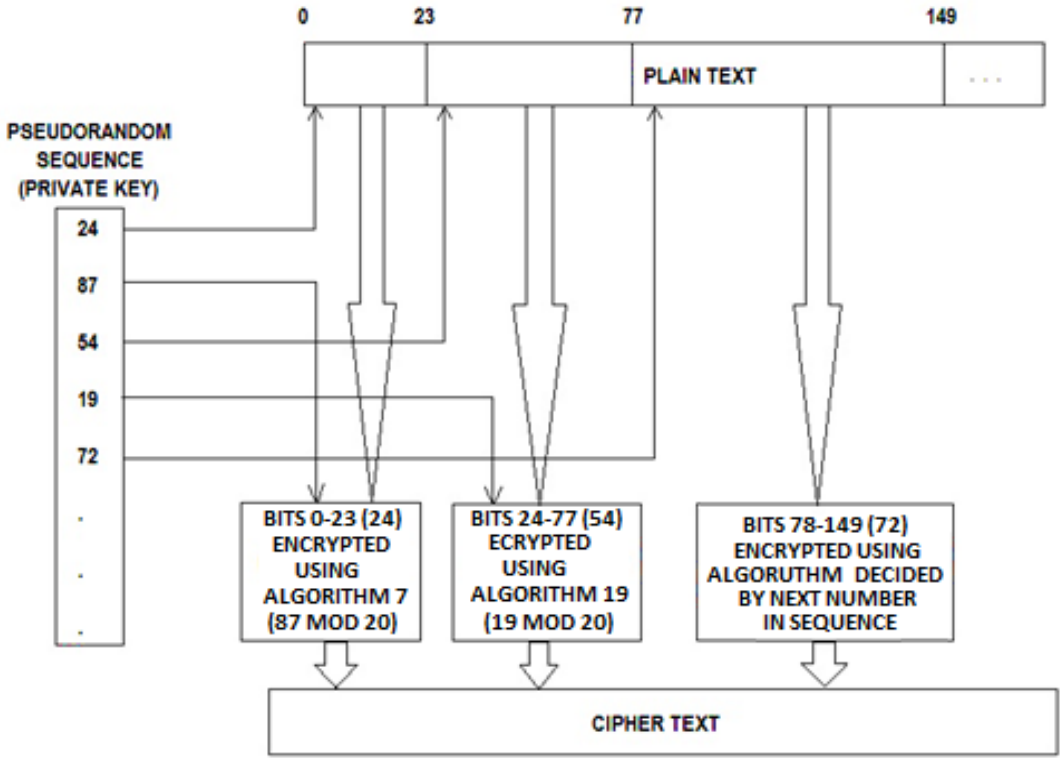

Fig. 1. Proposed Algorithm Hopping Symmetric Cryptography

III. BOOEAN FUNCTIONS AS ENCRYPTION ALGORITHM

The method in Fig. 1 is explained further by selecting Boolean functions as encryption algorithm. A pool of Boolean functions with different number of input is selected. Each of the Boolean function should have same number of inputs and outputs, so that it is bijective and there is equal number of encrypted bits for corresponding number of plain text bits. As an example, the truth table of bijective Boolean function with four inputs and four outputs is given in Table 1. The truth table in Table 1 is a one to one mapping between all the 16 combinations. The practical Boolean functions to perform the encryption will have many inputs and equal number of outputs.

The proposed hopping system takes first 24 bits of the plain text and encrypts using Boolean function 7, which produces 24 encrypted bits. Next 54 bits are encrypted using Boolean function 19, which again produces 54 bits and so on. The encrypted bits are then combined to form the cipher text which is transmitted to the receiver. Since the receiver knows the pseudorandom sequence and the Boolean function inverses, it can decrypt the cipher text. Though the encryption algorithms of Boolean functions are primitive, the mix with the hopping makes this method more secure.

IV. IMPLEMENTATION DETAILS

All of the cryptographic algorithms in literature are implemented and practiced. The proposed system with Boolean function as encryption/decryption algorithm (For example) can be implemented in C by building the BDD for Boolean function using CUDD [6]. The BDD built can be optimized using [7, 8, 9, 10, 11]. The optimized BDD can be converted to bit file and loaded in FPGA [12] and can be extended to ASIC [14].

V. ADVANTAGES, APPLICATIONS AND FUTURE WORK

[15] Provide methods to evaluate the performance of symmetric cryptographic algorithms. Since our implementation of the encryption algorithm is using simple Boolean functions, their realizations will be just logic gates. Hence the operation to perform encryption will be faster (in switching level) compared to other encryption schemes which rely upon intense decimal number operations.

The proposed encryption algorithm can be used in any system that needs security. One of the typical applications is [16].

The proposed system can be extended to asymmetric cryptography by adopting standard techniques [1]. Once applied, then it can be used by distributing the public key and need not worry about the safety in distributing the private key. This paper has

been successful publication in a conference [17].

Table 1: A Bijective Boolean Function

BOOLEAN FUNCTION							
INPUTS				**OUTPUTS**			
I	II	III	IV	I	II	III	IV
0	0	0	0	0	1	0	0
0	0	0	1	0	0	1	0
0	0	1	0	1	0	0	1
0	0	1	1	1	1	0	0
0	1	0	0	0	1	1	0
0	1	0	1	1	1	1	0
0	1	1	0	0	0	1	1
0	1	1	1	1	0	1	1
1	0	0	0	1	1	1	1
1	0	0	1	0	0	0	0
1	0	1	0	1	0	0	0
1	0	1	1	0	1	1	1
1	1	0	0	1	1	0	1
1	1	0	1	1	0	1	0
1	1	1	0	0	0	0	1
1	1	1	1	0	1	0	1

CONCLUSION

A novel algorithm hopping technique, for symmetric cryptography was introduced in this paper. The technique uses the concept of frequency hopping by using hopping pseudorandom sequence as private key to hop encryption algorithms. The technique

along with a Boolean function (as encryption algorithm) and implementation details was explained. The information provided with supporting details in section five proves that the proposed technique is efficient.

REFERENCES

[1] Menezes, Alfred J., Paul C. Van Oorschot, and Scott A. Vanstone. Handbook of applied cryptography. CRC press, 1996.

[2] Thakur, Jawahar, and Nagesh Kumar. "DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis." International journal of emerging technology and advanced engineering, Vol. 1, Issue 2, 2011, pp. 6-12.

[3] Brajal, Americo, and Antoine Chouly. "Multicarrier frequency hopping communications system." U.S. Patent No. 5,548,582. 20 Aug. 1996.

[4] Ephremides, Anthony, Jeffrey E. Wieselthier, and Dennis J. Baker. "A design concept for reliable mobile radio networks with frequency hopping signaling." Proceedings of the IEEE Vol. 75, Issue 1, 1987, pp. 56-73.

[5] Akers, Sheldon B. "Binary decision diagrams." IEEE Transactions on computers, Vol. 100, Issue 6, 1978, pp 509-516.

[6] Somenzi, Fabio. "CUDD: Colorado university decision diagram package," 1996.

[7] Raseen, Mohamed, PW Chandana Prasad, and Ali Assi. "An efficient estimation of the ROBDD's complexity." INTEGRATION, the VLSI journal, Vol. 39, Issue 3, 2006, pp. 211-228.

[8] Raseen, Mohamed, P. W. C. Prasad, and A. Assi. "Mathematical Model to Predict the Number of Nodes in an ROBDD." MWSCAS'04. Vol. 3, 2004, pp. 431-434.

[9] Prasad, P. W. C., et al. "BDD path length minimization based on initial variable ordering." Journal of Computer Science, Science Publications. Vol. 1, Issue 4, 2005, pp.521-529.

[10] Prasad, PW Chandana, Ali Assi, and Mohamed Raseen. "BDD minimization using graph parameter permutation." The 2004 International Conference on VLSI (VLSI 04), 2004, pp. 491-494.

[11] Prasad, P. W. C., M. Raseen, and S. Sasikumaran. "Delay minimization in pass transistor logic use of binary decision diagram." 2nd International Conference on Information Technology (ICIT 2005). 2005.

[12] Pellerin, David, and Scott Thibault. "Practical FPGA programming in C". Prentice Hall Press, 2005.

[13] Stark, Emily, Michael Hamburg, and Dan Boneh. "Symmetric cryptography in javascript." Computer Security Applications Conference, 2009. ACSAC'09. Annual. IEEE, 2009.

[14] Wolkerstorfer, Johannes, Elisabeth Oswald, and Mario Lamberger. "An ASIC implementation of the AES SBoxes." Cryptographers' Track at the RSA Conference. Springer Berlin Heidelberg, 2002.

[15] Singh, Gurjeevan, Ashwani Kumar Singla, and K. S. Sandha. "Performance evaluation of symmetric cryptography algorithms." International Journal of Electronics and Communication Technology Vol. 2, Issue 3, 2011, pp. 141-146.

[16] Azzaz, Mohamed Salah, et al. "Synchronized hybrid chaotic generators: Application to real-time wireless speech encryption." Communications in Nonlinear Science and Numerical Simulation Vol. 18, Issue 8, 2013, pp. 2035-2047.

[17] M. Raseen, Moh'd Radaideh, "Algorithm Hopping Symmetric Cryptography", IASTEM International Conference, Kuala Lumpur, Malaysia, 2017, pp.32-34.

AUTHOR'S PROFILE

Dr. Mohamed Raseen

Affiliation : Independent Consultant

Email : dr.raseen@gmail.com

Dr. Raseen has a PhD from, Anna University, India, MS from UHCL, USA and BE from Bharathiar University, India. His research areas are Binary Decision Diagrams, Genetic Algorithms, Cryptography and E-Health. He has published 11 research papers in International Journals and 26 research papers in International Conferences. His publications are cited by 8 US Patents and 108 Research Papers

Dr. Moh'd Radaideh

Affiliation : Department of Software Engineering, Amman Arab University

Email : Radaideh@aau.edu.jo

Dr. Radaideh is currently an Associate Professor of Software Engineering at the Faculty of Informatics of the Amman Arab University (AAU), serving in the Capacity of Chairman of the Departments of Software Engineering and Mobile Computing as well as in the capacity of Assistant President for

International Relations. Dr. Radaideh holds a Ph.D. in Electrical and Computer Engineering / Specialized in Software Engineering from McMaster University of Hamilton in Canada (YR2000), a Masters Certificate in Project Management from George Washington University (YR2000), a Master Degree in Electrical and Computer Engineering from Jordan University of Science and Technology (YR1989), and a Bachelor Degree in Electrical and Computer Engineering from Yarmouk University (YR1987) in Jordan. Dr. Radaideh spent several years in the Software Industry leading teams, architecting, designing, and/or implementing web and enterprise solutions that involved search technologies, database management systems, web servers, web application servers, etc. Dr. Radaideh developed many Java-based integration components that are currently used to integrate various web tools. Dr. Radaideh has been a professional member of the ACM, and a member of the IEEE (membership shall be renewed soon).