International Journal of Advance Research in Science and Engineering
Volume No.06, Special Issue No.(01), December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

Encryption Techniques and Application of Boolean Functions in Cryptography

Jinamul Hasan Khan[1], Dr. Sonal Bharti[2], Dr. Deep Singh[3]

[1]Department of Mathematics, Sri Satya Sai University of Technology and Medical Sciences Bhopal Madhya Pradesh (India)

[2]Head, Department of mathematics, Sri Satya Sai University of Technology and Medical Science, Bhopal Madhya Pradesh (India)

[3]Assistant Professor, Department of Mathematics, Central University of Jammu, J&K State, (India).

ABSTRACT

Cryptography is a popular ways of sending synergistic information in secret way. There are many cryptographic techniques available and among them Boolean function is one of the most powerful techniques to protect data from unauthorized parties. Boolean functions are the process of reducing the effect of the hackers in cyber crimes. The security of communication is a very important issue on World Wide Web. Digital information is stored data which provide protection of assets. Data security refers to protective digital privacy measures that are applied to protect unauthorized access to computers, personal databases and websites. Cryptography protects users by providing functionality for the encryption of data and authentication of other users.

Keywords*: *Boolean function, Block cipher, Cryptography Encryption, Synergistic, Stream cipher.

I. INTRODUCTION

Nowadays most of the Business, Trade, Production, Defense, Educational, Research and Development (R&D), Management, Organizations of the world, uses Computers on a very large scale. Privacy is the critical issue to protect data from unauthorized users. Cryptography plays a major role to encrypt data [1].Cryptography is the science of protecting data, provides methods of converting data into inaccessible form, so that only an authorized user (s) can access data / information at the destination. Cryptography is the science of using mathematics to encrypt and decrypt data. Modern cryptography is majorly based on theories of mathematics and computer science. For secure communication over a public channel, we need some algorithms and protocols [2]. According to Shannon to get secure transmission of piece of information it is sufficient to obtain some efficient encryption algorithms. In general, these encryption algorithms have extensive use of Boolean functions [3].Thus the aim of this articles is to provides updated information on cryptography encryption and analysis of Boolean function.

II. DATA ENCRYPTION

Data encryption is a process of random string of bits created clearly for scrambling and unscrambling data. Data encryption consists algorithms intended to insure that every key is unpredictable and unique. There are two types of keys in cryptography; symmetric and asymmetric. Symmetric keys have been around the longest; they use a single key for both the encryption and decryption of cipher text. This type of key is termed as secret key. Secret key ciphers generally classified into one of the two categories: Stream ciphers or Block ciphers. A Block cipher applies a private key and algorithm to a block of data simultaneously, where as a Stream cipher applies the key and algorithm one bit at a time. Most crypto graphical techniques use symmetric encryption to encrypt data transmissions but use asymmetric encryption to encrypt and exchange the secret key [4, 5].

III. BOOLEAN FUNCTIONS AND ITS APPLICATION IN CRYPTOGRAPHY

A Boolean function on n-variables is a function from Z_2n to Z_2, where Z_2 is a prime field of characteristic 2 and Z_2n is n degree extension field of Z_2.Boolean functions have applications in various fields like circuit theory, coding theory, cryptography. They are central objects in the design and security of cryptosystems (stream ciphers and block ciphers) [6].. A cryptosystem is an algorithm required to implement special types of encryptions and decryptions. The protection of cryptosystems against various cryptographic attacks is strongly related to the properties of Boolean functions such as nonlinearity, balancedness, resiliency, cross correlation, algebraic immunity and higher-order nonlinearity [7]. The Boolean functions used in various cryptosystems should satisfy various cryptographic criteria. However, it is impossible to optimize all the criteria simultaneously, so there are some trades among these criteria. According to the application, one has to decide that which criteria are more important. For example, for the pseudo randomness of key stream, the functions employed in the stream ciphers should be balanced. Boolean functions can be employed either as combiner functions or as filter functions in stream ciphers based on linear feedback shift register (LFSR) [8]. The Boolean functions used in stream ciphers as a combiner function should possess high nonlinearity to prevent the system from linear approximation attack. Higher-order nonlinearity (nl_r) is the generalization of the notion of nonlinearity [9]. In 2008, Carlet has done a pioneer work on higher-order nonlinearity and obtained lower bounds on (nl_r) in the recursive framework. He derived lower bounds on (nl_r) for several classes of Boolean functions such as inverse functions, Welch functions, Kasami functions and the functions in Maiorana-Mcfarland (MMF) bent class [10]

IV. CONCLUSION

Boolean function offers an attractive approach for prevent data. It is modern technology in cryptography which encrypt information into unreadable form of data, whereby hackers and unauthorized person cannot access my secret information.

V. ACKNOWLEDGMENTS

I would like to express my special thanks of gratitude to my teacher Dr.Abdul Salam, Dr.S.Mujeebuddin as well as our colleague Asst.Prof.Aman Agarwal who gave me the golden opportunity to do this valuable research paper on the topic "Encryption Techniques and Application of Boolean Functions in Cryptography" which also helped me doing a lot of research and I came to know about so many new things secondly I would also like to thanks my parents and friends who helped me a lot in finalizing this research paper.

REFERENCES

[1.] Biham E. and Shamir A.: Differential cryptanalysis of DES-like cryptosystems, In Advance in cryptography CRYPTO 1990, Lecture Notes in Computer Science, Springer-Verlag, Vol. 537, pp. 2-21, 1991.

[2.] Carlet C.: On the higher order nonlinearities of algebraic immune functions, In CRYPTO 2006, Lecture Notes in Computer Science, Springer-Verlag, Vol. 4117, pp. 584-601, 2006.

[3.] Shannon C., Communication theory of secrecy systems, Bell System Technical Journal Vol.28, pp. 656-715, 1949.

[4.] International journal of engineering and computer scinces ISSN:2319-7242. Vol.6 issue 4 april 2017,pp 20915-20919.

[5.] Courtois N.: Fast algebraic attacks on stream ciphers with linear feedback, In Advance in Cryptography CRYPTO 2003, Lecture Notes in Computer Science, Springer-Verlag, Vol. 2729, pp. 176-194, 2003.

[6.] Gode R. and Gangopadhyay S.: Third-order nonlinearities of a subclass of Kasami functions, Cryptography and Communications - Discrete Structures, Boolean functions and Sequences, Vol. 2, pp. 69-83, 2010.

[7.] Iwata T. and kurosawa K.: Probabilistic higher order differential attack and higher order bent functions, In Proceedings of the ASIACRYPT 1999, Lecture Notes in Computer Science, Springer-Verlag, Vol. 1716, pp. 62-74, 1999.

[8.] Singh D.: Second-order nonlinearities of some classes of cubic Boolean functions based on secondary constructions, International Journal of Computer Science and Information Technologies, Vol. 2 (2) , pp. 786-791, 2011.

[9.] Matsui M.: Linear cryptanalysis method for DES cipher, In proceedings of the EUROCRYPT 1993, Lecture Notes in Computer Science, Vol. 765, pp. 386-397, 1994.

[10.] Carlet C.: Recursive lower bounds on the nonlinearity profile of Boolean functions and their applications, IEEE Trans. Inform. Theory, Vol. 54 (3), pp. 1262-1272, 2008.