

Chapter 15

Complexity Measures of Cryptographically Secure Boolean Functions

Chungath Srinivasan

Amrita Vishwa Vidyapeetham, India

Lakshmy K.V.

Amrita Vishwa Vidyapeetham, India

M. Sethumadhavan

Amrita Vishwa Vidyapeetham, India

ABSTRACT

Boolean functions are used in modern cryptosystems for providing confusion and diffusion. To achieve required security by resistance to various attacks such as algebraic attacks, correlation attacks, linear, differential attacks, several criteria for Boolean functions have been established over years by cryptographic community. These criteria include nonlinearity, avalanche criterion and correlation immunity and the like. The chapter is an attempt to present state of the art on properties of such Boolean functions and to suggest several directions for further research.

1. INTRODUCTION

In stream cipher cryptography a pseudorandom sequence of bits of length equal to the message length is generated. This sequence is then bitwise XORed (addition modulo 2) with the message sequence and the resulting sequence is transmitted. At the receiving end, deciphering is done by generating the same pseudorandom sequence and bitwise XORing the cipher bits with the random

bits. The seed of the pseudorandom bit generator is obtained from the secret key. For some recent proposals of stream ciphers refer the eSTREAM Project (The ECRYPT Stream Cipher Project). Linear (non-linear) Feedback Shift Registers (LFSRs) and Boolean functions are important building blocks for stream cipher systems. A standard model of stream cipher by Siegenthaler (1984, 1985) combines the outputs of several independent LFSR sequences using a nonlinear Boolean function to produce the keystream. Design and analysis of stream ciphers was kept

DOI: 10.4018/978-1-60960-123-2.ch015

confidential for a long time and was made public in the 1970's, when several research papers on the design of LFSR-based stream ciphers occurred. Cryptanalysis techniques discovered during the NESSIE and eSTREAM projects (Bernstein (Report 2008/010), The ECRYPT Stream Cipher Project) have made it possible to strengthen cipher designs to a large extent, and attacking new algorithms has become more difficult. Till the end of 1990's there are no standards for stream ciphers and the advent of these projects standardized the design of stream ciphers (Chris & Alexander 2004, The ECRYPT Stream Cipher Project). An LFSR is essentially an elementary algorithm for generating a keystream, which has the following desirable properties:

- Easy to implement in hardware.
- Produce sequences of long and deterministic period.
- Produce sequences with good statistical properties.
- Can be readily analyzed using algebraic techniques.

In this chapter section 2 gives an insight into Boolean functions and its different forms of representations, section 3 gives details of different complexity measures that a Boolean functions has to satisfy, section 4

2. BOOLEAN FUNCTIONS

Boolean functions play a central role in preserving the security of stream ciphers and block ciphers. Let n be any positive integer. We denote by B_n the set of all n -variable Boolean functions from the vector space F_2^n of binary vectors of length n to F_2 . We denote \oplus by the additions in F_2 . The representation of Boolean functions which is mostly used in cryptography is the algebraic normal form (ANF) as given in Equation (2.1) and the truth table representation (TT):

$$f(x_1, x_2, \dots, x_n) = \bigoplus_{u \in F_2^n} a_u x^u, \quad a_u \in F_2, \quad x, u \in F_2^n \quad (2.1)$$

The unique degree of ANF for a Boolean function is called the algebraic degree of the function. The Boolean functions whose algebraic degrees do not exceed 1 are called the affine functions. The TT of an n variable Boolean function is the 2^n length bit binary sequence obtained from the output of a Boolean function. There are also algorithms for getting one form of representation of Boolean functions from its other form of representation. The Trace representation of a Boolean function also plays a vital role in studying and defining these functions. The trace function $tr: F_2^n \rightarrow F_2$ is defined as $tr(x) = x + x^2 + x^{2^2} + \dots + x^{2^{n-1}}$. Every Boolean function f can be written in the form $f(x) = tr(F(x))$ where F is a mapping from F_2^n into F_2^n . The numerical normal form (NNF) representation of Boolean functions is not discussed in this chapter. The sign function of a Boolean function f is defined as $(-1)^f$.

The Walsh Transform of a function f on F_2^n is the map $W_f: F_2^n \rightarrow \mathbb{R}$ (set of real numbers), defined by:

$$W_f(a) = \sum_{x \in B_n} (-1)^f (-1)^{a \cdot x}, \quad (2.2)$$

where $a \cdot x = a_1 x_1 \oplus a_2 x_2 \oplus \dots \oplus a_n x_n$. The non-linearity of f is:

$$NL(f) = 2^{n-1} - \frac{1}{2} \max_{a \in F_2^n} |W_f(a)| \quad (2.3)$$

Parseval's equation:

$$\sum_{a \in F_2^n} (W_f(a))^2 = 2^{2n} \quad (2.4)$$

9 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/complexity-measures-cryptographically-secure-boolean/50724

Related Content

A Scheme for Face Recognition in Complex Environments

Wei Cui and Wei Qi Yan (2016). *International Journal of Digital Crime and Forensics* (pp. 26-36).

www.irma-international.org/article/a-scheme-for-face-recognition-in-complex-environments/144841

CloudIoT: Towards Seamless and Secure Integration of Cloud Computing With Internet of Things

Junaid Latief Shah, Heena Farooq Bhat and Asif Iqbal Khan (2019). *International Journal of Digital Crime and Forensics* (pp. 1-22).

www.irma-international.org/article/cloudiot/227637

Evaluation of Autopsy and Volatility for Cybercrime Investigation: A Forensic Lucid Case Study

Ahmed Almutairi, Behzad Shoarian Satari, Carlos Rivas, Cristian Florin Stanciu, Mozhdeh Yamani, Zahra Zohoor Saadat and Serguei A. Mokhov (2020). *International Journal of Digital Crime and Forensics* (pp. 58-89).

www.irma-international.org/article/evaluation-of-autopsy-and-volatility-for-cybercrime-investigation/240651

Control Systems Security

Jake Brodsky and Robert Radvanovsky (2011). *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (pp. 187-204).

www.irma-international.org/chapter/control-systems-security/46426

Human Detection and Intelligent Action Recognition for Automatic Visual Surveillance and Monitoring Systems: Its Current Trends

Lakhyadeep Konwar, Navajit Saikia and Subhash Chandra Rajbongshi (2026). *Advancements in Forensic Analysis of Digital Images for Security and Law Enforcement* (pp. 227-278).

www.irma-international.org/chapter/human-detection-and-intelligent-action-recognition-for-automatic-visual-surveillance-and-monitoring-systems/400204