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):

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

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 $tr(x) = x + x^2 + x^{2^2} + ... + x^{2^{n-1}}$. 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: $F_2^n \rightarrow$ R (set of real numbers), defined by:

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

where $a.\ x = a_1x_1 \oplus a_2x_2 \oplus ... \oplus a_nx_n$. The nonlinearity of f is:

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

Parseval's equation:

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