Topics in Coding, Cryptography and Information Security

Editors:

Mohammad Umar Siddiqi
Sigit Puspito Wigati Jarot
Othman Omran Khalifa

IIUM PRESS
2011

Topics in Coding, Cryptography and Information Security

Editors:

Mohammad Umar Siddiqi
Sigit Puspito Wigati Jarot
Othman Omran Khalifa

IIUM Press
2011

Published by:
IIUM Press
International Islamic University Malaysia

First Edition, 2011

Perpustakaan Negara Malaysia Cataloguing-in-Publication Data

Mohammad Umar Siddiqi, Sigit Puspito Wigati Jarot and Othman Omran Khalifa: Topics in Coding, Cryptography and Information Security

ISBN: 978-967-418-169-7

Member of Majlis Penerbitan Ilmiah Malaysia – MAPIM
(Malaysian Scholarly Publishing Council)

Printed by :
IIUM PRINTING SDN. BHD.
No. 1, Jalan Industri Batu Caves 1/3
Taman Perindustrian Batu Caves
Batu Caves Centre Point
68100 Batu Caves
Selangor Darul Ehsan

Topics in Coding, Cryptography and Information Security

Contents

PART III: CRYPTOGRAPHY AND INFORMATION SECURITY

Chapter 13

Cryptographic Boolean Functions: Transform Domain Perspective

Hashum Mohamed Rafiq and Mohammad Umar Siddiqi

13.1. Introduction

This chapter examines the main properties of cryptographic Boolean functions and looks at various representation methods that have been employed to study and utilize them so far. A sequel to this is to address an alternative approach that can be used as an alternative tool in analyzing and manipulating such functions.

Boolean functions have been of great interest in many fields of engineering and science, especially in cryptography [1]. Most modern conventional cryptographic systems are based on the notion of product ciphers [2] which represent a class of cryptosystems that iterate a composite operation to map plaintext to cipher-text. Each such iteration is known as a round of the cipher and consists of a combination of transposition and substitution operation. The combination of such operations can produce a cryptographically strong nonlinear mapping when applied a sufficient number of times [3]. Each round consists of an application of a transposition and a substitution derived from a set of fixed auxiliary tables (S-boxes), guided by the sub-key for that round. Given that transposition is a linear operation, then the substitution operation is the only source of nonlinearity in the cipher and therefore the security [4].

As the S-boxes provide the security in these cryptosystems, their design is of critical importance. However, since 1985, the research attention shifted to Boolean functions, which can be viewed as component parts of an S-box, and to define and analyzing their properties [4]. The initial design properties or criteria for the Boolean functions include: balance, nonlinearity [5], non-degeneracy/completeness [6], correlation immunity [7], satisfy the strict avalanche criterion (SAC) [8], or be bent [9]. These properties may be collectively referred to as nonlinearity criteria [5, 10] and can be extended in several natural ways. For example, functions may be chosen so that they achieve a maximum distance from all functions that are affine [5] or have linear structures [11, 12] which are considered cryptographically weak. Also the nonlinearity criterion can be considered to be robust if it is invariant under certain simple mappings such as affine transformation. In [5], it was shown that the distance to the set of linear functions, and the nonlinear order of a function [13] are both invariant under non-singular linear transformation.

A property P, such as nonlinearity, in a function may be considered stronger in the function if P is still retained when certain subsets of the input bits are held