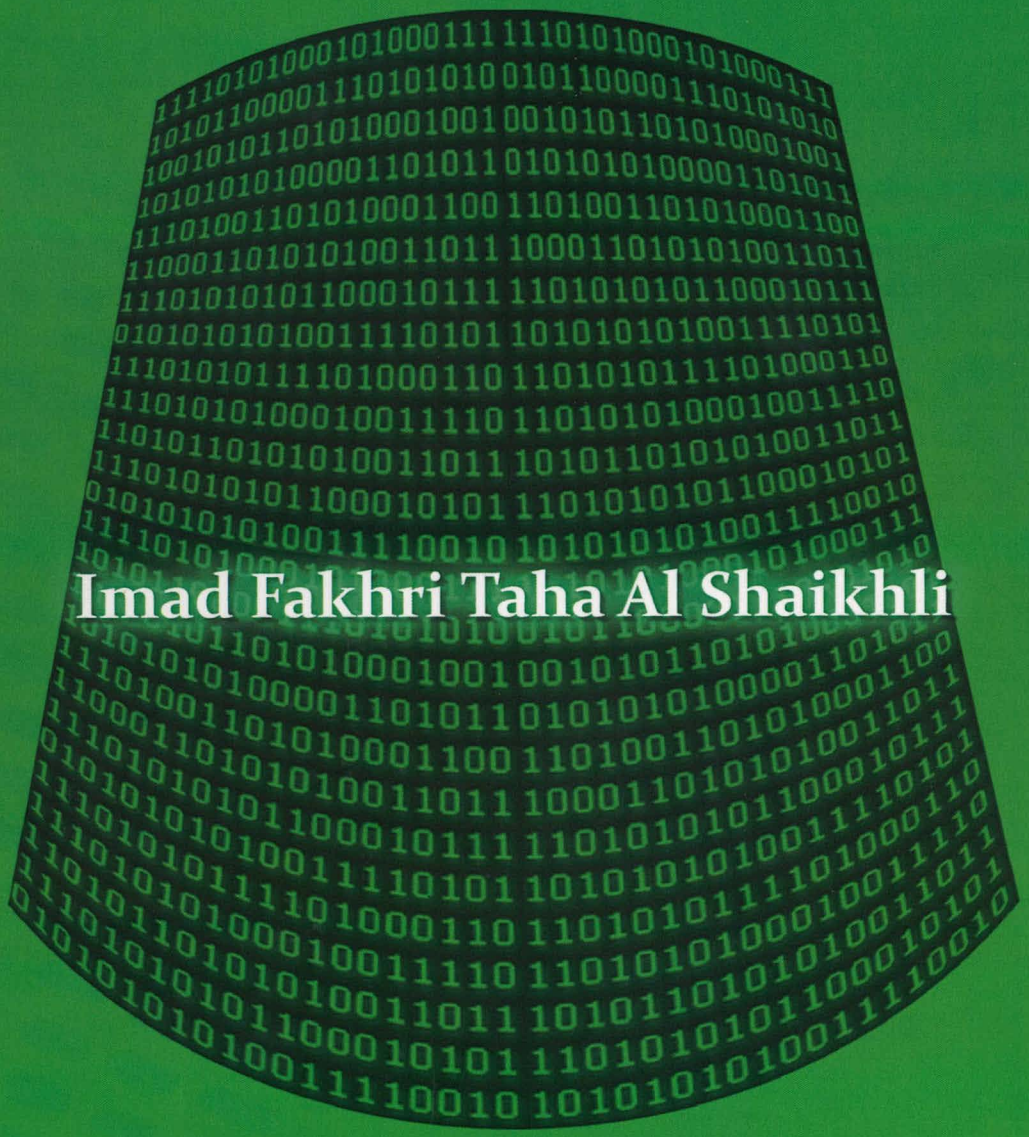
Cryptography

Past, Present and Future

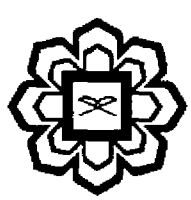


Imad Fakhri Taha Al Shaikhli

IIUM PRESS
INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

Cryptography: Past, Present and Future

Imad Fakhri Taha Al Shaikhli



IIUM Press

Published by:

IIUM Press

International Islamic University Malaysia

First Edition, 2011

Perpustakaan Negara Malaysia Cataloguing-in-Publication Data

Imad Fakhri Taha Al-Shaikhli
Cryptography: Past, Present and Future
Imad Fakhri Taha Al-Shaikhli

ISBN: 978-967-418-091-1

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

TABLE OF CONTENTS

- Sibomana Hilali Hussein

17. Interactive Proof Systems

- Rusydi Hasan
- Imad Fakhri Taha Al Shaikhli
- Siti Khairunnisa Mohd Bakri
- Nur Dalilah Bt More Yusoff
- Nur Khairunnisa Bt Juarah

ABSTRACT

In this article we will talk about the background of Interactive Proof Systems. Also we will introduce into definition of interactive turing machine and Proof Systems. Also, we will give examples.

BACKGROUND

Interactive proof systems have been introduced by Goldwasser, Micali and Rackoff [GMR85] and Babai [Ba85] independently in 1985. The idea of interactive proof systems extends the idea of efficient proofs which has led to the class IP. Interactive proof systems are a randomized extension to NP formalization of the concept of an efficient proof system captures one way of communicating a proof. There is a deterministic polynomial-time verifier (in the length of the common input) that will exchange the messages (strings) with an infinitely powerful prover which will persuade the verifier to be convinced of the truth of a proposition with a very small probability error. Interactive Turing machines will be defined below before defining interactive proof systems further. (Mohr, 2011)