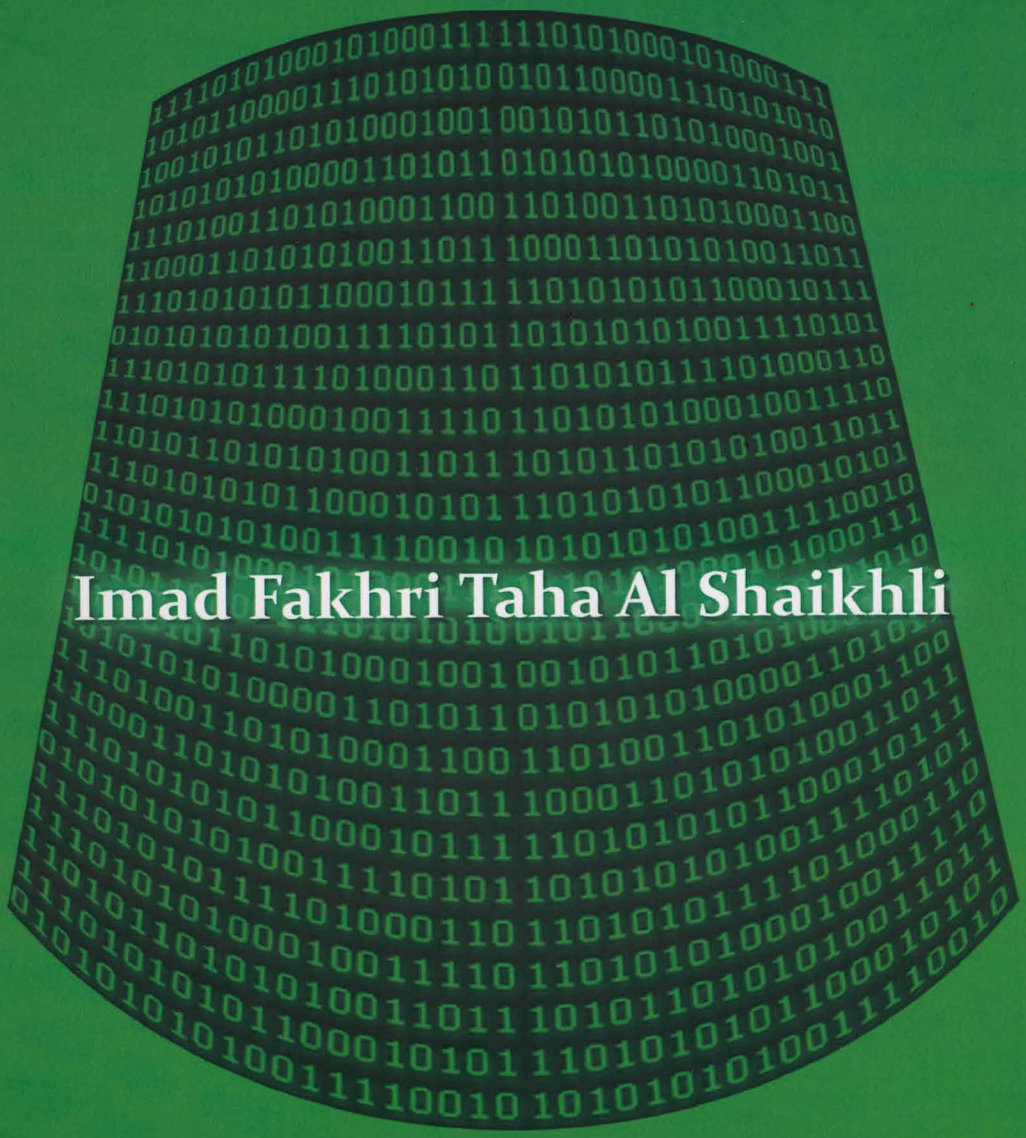
Cryptography

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

Chapter 23

Quantum cryptography

Abstract

Quantum cryptography offers a secure communication between two parties against eavesdroppers with unlimited computing power. It is based on physical laws and does not rely upon any complexity assumptions. This chapter presents some mathematical foundation for the study of quantum cryptography which will be of great help to understand how the first quantum cryptography named BB84 works. Before going into details, we shall first introduce the postulates of quantum physics.