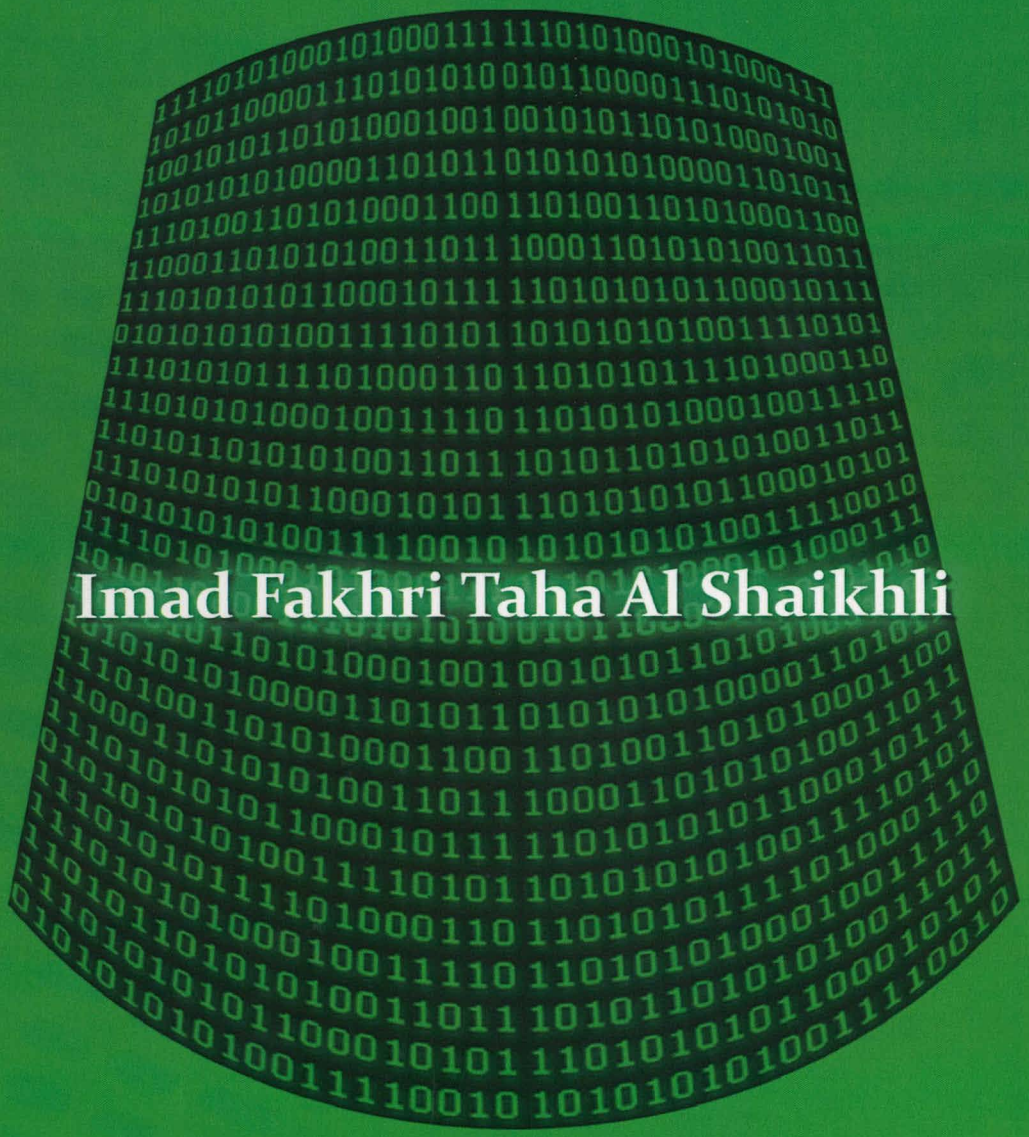
Cryptography

Past, Present and Future

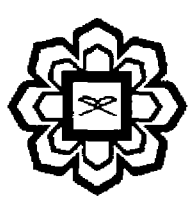


Imad Fakhri Taha Al Shaikhli

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

22. Blakely's Secret Sharing Scheme

- Sufyan Salim Mahmood Al Dabbagh
- Imad Fakhri Taha Al Shaikhli
- Muhammad Israfil

ABSTRACT

Function sharing deals with the problem of distribution of the computation of a function (such as decryption or signature) among several parties. The necessary values for the computation are distributed to the participating parties using a secret sharing scheme. Several function sharing schemes have been proposed in the literature, with most of them using Shamir secret sharing as the underlying Secret Sharing Scheme. In this paper, we investigate how threshold cryptography can be conducted with Blakely secret sharing scheme and present a novel function sharing scheme for the RSA cryptosystem. The challenge is that constructing the secret in Blakely's Secret Sharing Scheme requires the solution of a linear system which normally involves computing inverses, while computing inverses modulo $\varphi(N)$ cannot be tolerated in a threshold RSA system in any way.

BACKGROUND

Blakely's secret sharing scheme is geometric in nature (Blakeley, 1979). The secret is a point in an m-dimensional space. n shares are constructed with each share defining a hyperplane in this space. By finding the intersection of any m of these planes, the secret (or point of intersection) can be obtained. This scheme is not perfect, as the person with a share of the secret knows that the secret is a point on his hyperplane. Nevertheless, this scheme can be modified to achieve perfect security (Simmons, 1992).