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
TABLE OF CONTENTS

Dedication 1
Preface VII
Acknowledgement VIII

PART I Classical Cryptography 1

Chapter One Introduction 3-9
- Imad Fakhri Taha Al Shaikhli
- Rusydi Hasan
- Nurhidayah Binti Abdulrahid
- Faizurimawaty Bt Padzilah
- Nabilah Bt Abd Rahman

Chapter Two Monoalphabetic Substitution Cipher 11-16
- Imad Fakhri Taha Al Shaikhli
- Rusydi Hasan
- Nurhidayah Binti Abdulrahid
- Faizurimawaty Bt Padzilah
- Nabilah Bt Abd Rahman

Chapter Three Polyalphabetic Substitution Cipher 17-23
- Imad Fakhri Taha Al Shaikhli
- Rusydi Hasan
- Nurhidayah Binti Abdulrahid
- Faizurimawaty Bt Padzilah
- Nabilah Bt Abd Rahman

Chapter Four Machine-Based Cryptography 25-30
- Rusydi Hasan
- Imad Fakhri Taha Al Shaikhli
- Nurhidayah Binti Abdulrahid
- Faizurimawaty Bt Padzilah
- Nabilah Bt Abd Rahman

PART II Modern Symmetric-Key Cryptography 31

Chapter Five Block and Stream Cipher 33-38
- Sufyan Salim Mahmood Al Dabbagh
- Imad Fakhri Taha Al Shaikhli
- Muhammad Fadil Lubis
- Usman bin Mohd Azhar
- Nopan Ziro Ando

Chapter Six Data Encryption Standard (DES) 39-46
- Imad Fakhri Taha Al Shaikhli
- Sufyan Salim Mahmood Al Dabbagh
- Muhammad Fadil Lubis
- Usman bin Mohd Azhar
- Nopan Ziro Ando

**Chapter Seven Advanced Encryption Standard (Rijndael)**  
- Sufyan Salim Mahmood Al Dabbagh
- Imad Fakhri Taha Al Shaikhli
- Muhammad Fadil Lubis
- Usman bin Mohd Azhar
- Nopan Ziro Ando

**Chapter Eight Trivium and Rabbit Stream Cipher**  
- Imad Fakhri Taha Al Shaikhli
- Sufyan Salim Mahmood Al Dabbagh
- Muhammad Fadil Lubis
- Usman bin Mohd Azhar
- Nopan Ziro Ando

**PART III Hash Functions**  

**Chapter Nine Introduction**  
- Khanssaa Munthir Abdulmajed
- Imad Fakhri Taha Al Shaikhli
- Sufyan Salim Mahmood Al Dabbagh
- Ahmad Faridi Abdul Matin
- Sibomana Hilali Hussein

**Chapter Ten Message Digest (MDX) Family**  
- Imad Fakhri Taha Al Shaikhli
- Sufyan Salim Mahmood Al Dabbagh
- Khanssaa Munthir Abdulmajed
- Ahmad Faridi Abdul Matin
- Sibomana Hilali Hussein

**Chapter Eleven SHA family hash function**  
- Khanssaa Munthir Abdulmajed
- Imad Fakhri Taha Al Shaikhli
- Sufyan Salim Mahmood Al Dabbagh
- Ahmad Faridi Abdul Matin
- Sibomana Hilali Hussein

**Chapter Twelve RIPEMD and Chameleon Hash Function**  
- Sufyan Salim Mahmood Al Dabbagh
- Imad Fakhri Taha Al Shaikhli
- Khanssaa Munthir Abdulmajed
- Ahmad Faridi Abdul Matin
PARTIV Public Key & Digital Signature Schemes

Chapter Thirteen Rivest-Shamir-Adleman (RSA)
- Iqram Mohammed Hayek
- Imad Fakhri Taha Al Shaikhli
- Sufyan Salim Mahmood Al Dabbagh
- Kusai Abu Hilal

Chapter Fourteen Cryptanalysis of RSA
- Imad Fakhri Taha Al Shaikhli
- Sufyan Salim Mahmood Al Dabbagh
- Iqram Mohammed Hayek
- Kusai Abu Hilal

Chapter Fifteen Digital Signature Algorithm
- Sufyan Salim Mahmood Al Dabbagh
- Imad Fakhri Taha Al Shaikhli
- Iqram Mohammed Hayek
- Kusai Abu Hilal

Part V Zero-Knowledge Proof

Chapter Sixteen Background of Zero-Knowledge Proof
- Imad Fakhri Taha Al Shaikhli
- Rusydi Hasan
- Siti Khairunnisa Mohd Bakri
- Nur Dalilah Bt More Yusoff
- Nur Khairunnisa Bt Juarah

Chapter Seventeen Interactive Proof Systems
- Rusydi Hasan
- Imad Fakhri Taha Al Shaikhli
- Siti Khairunnisa Mohd Bakri
- Nur Dalilah Bt More Yusoff
- Nur Khairunnisa Bt Juarah

Chapter Eighteen Zero-Knowledge Proof
- Imad Fakhri Taha Al Shaikhli
- Rusydi Hasan
Chapter Nineteen Feige-Fiat-Shamir Identification Scheme
- Rasydi Hasan
- Imad Fakhri Taha Al Shaikhli
- Siti Khairunnisa Mohd Bakri
- Nur Dalilah Bt More Yusoff
- Nur Khairunnisa Bt Juarah

Part VI Secret Sharing

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

Chapter Twenty One Shamir’s Threshold Scheme
- Imad Fakhri Taha Al Shaikhli
- Sufyan Salim Mahmood Al Dabbagh
- Muhammad Israfil

Chapter Twenty Two Blakely’s Secret Sharing Scheme
- Sufyan Salim Mahmood Al Dabbagh
- Imad Fakhri Taha Al Shaikhli
- Muhammad Israfil

Part VII Quantum Cryptography

Chapter Twenty Three Quantum Cryptography
- Azeddine Messikh
18. Zero-Knowledge-Proof

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

ABSTRACT

In this article we will talk about the background of variant of zero-knowledge proof.

Also we will introduce into perfect and statistical of zero-knowledge proof. Moreover, we will describe the Computational of zero-knowledge proof.

BACKGROUND

Zero-Knowledge proofs are interactive proofs system \((P, V)\) that yield nothing (to the verifier) beyond the fact that the assertion is indeed valid. Whenever \(x \in L\), the verifier is able to generate on its own the conversations it could have had with the prover during an interactive proof of \(x \in L\). The verifier learns nothing as the result of a conversation with the prover that it could not have learned on its own by generating the conversation itself other than the fact that \(x \in L\). Zero-Knowledge proofs exhibit an extreme contrast between being convinced of the validity of the message and learning anything in addition (while receiving such convincing proof). A fundamental result regarding the zero-knowledge proof systems is their existence, under reasonable complexity assumptions, for any set in \(\text{NP}\) and it is presented for the Graph 3-Colorability. Suppose the prover wish to convince the verifier that a certain input graphis three-colorable, without revealing to the verifier the coloring that the prover knows. The prover can do so in a sequence of \(|E|^2\) stages, each of which goes as follows. (Micciancio, 2003)