

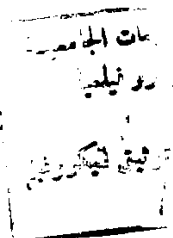
AIN SHAMS UNIVERSITY  
Faculty of Science  
Mathematics Department

**THEORY AND APPLICATION OF  
ZERO-KNOWLEDGE  
PROOFS**



BY  
**MAGED MOHAMED ABD EL-LATIF ELGENDY**  
Research Development Centre  
NATIONAL DEFENCE COUNCIL

THESIS  
SUBMITTED FOR THE DEGREE  
OF  
DOCTOR OF PHILOSOPHY IN SCIENCE  
(Pure Mathematics)



Supervised by

**Prof. Dr. Bayoumi I. Bayoumi**  
Department of Mathematics,  
Faculty of Science,  
Ain Shams University

**Dr. Mohamed M. Kouta**  
Department of Computer Science and  
Operations Research,  
Military Technical College

M. Kouta

**Dr. Fathy S. Holail**  
Head of C.R. Division  
Research Development Centre  
National Defence Council

Fathy S. Holail

1996







## CONTENTS

	Page
ACKNOWLEDGEMENT .....	i
SUMMARY .....	ii-vi
ABSTRACT .....	vii
CHAPTER 1 <i>Complexity-Theoretic Foundations of Cryptography</i> .....	1
1.1 The Theory of Resource-Bounded Computations .....	2
1.1.1 Introduction .....	2
1.1.2 Deterministic Polynomial-Time Computations .....	4
1.1.3 Nondeterministic Polynomial-Time Computations .....	4
1.1.4 Probabilistic Polynomial-Time Computations .....	7
1.1.5 One-Way Functions .....	7
1.1.6 Indistinguishability of Random Variables .....	9
1.1.7 Pseudo-Random Generators .....	11
1.1.8 Deterministic and Nondeterministic Public-Key Cryptosystems .....	12
1.1.8.1 Trap-door, One-way Functions .....	13
1.1.8.2 Deterministic Public-Key Cryptosystems .....	14
1.1.8.3 Nondeterministic Public-Key Cryptosystems ..	15
1.2 The Theory of Average-Case Complexity .....	17
1.2.1 Introduction .....	17
1.2.2 Average Case Intractability of Complete Problems .....	17
1.2.2.1 Randomized Tiling Problem .....	19
1.2.3 Polynomial Time Solvability for Some NP-Complete Languages on Average .....	20

1.2.3.1 Randomized Hamiltonian Circuits with Edge Probability $p$ .....	21
1.2.3.2 Randomized Graph-3Colouring .....	21
1.2.3.3 Randomized Subset Sum Problem .....	21
1.2.3.4 Randomized 3-Satisfiability Problem .....	22
<b>CHAPTER 2 <u>Zero-Knowledge Proofs</u></b> .....	23
2.1 Zero-Knowledge Proof Systems .....	24
2.1.1 Introduction .....	24
2.1.2 Minimum and Maximum Disclosure Proofs .....	25
2.1.3 Interactive Proof Systems .....	26
2.1.3.1 An interactive Proof System for Quadratic Nonresiduosity .....	30
2.1.3.2 An Interactive Proof System for Graph Nonisomorphism .....	30
2.1.4 Zero-Knowledge Interactive Proof Systems .....	32
2.1.4.1 A Zero-Knowledge Interactive Proof for Graph Isomorphism .....	34
2.1.5 Zero-Knowledge Interactive proof Systems for All NP-Languages .....	38
2.2 Zero-Knowledge Proofs of Knowledge .....	42
2.2.1 Introduction .....	42
2.2.2 Zero-Knowledge Interactive Proofs of Knowledge .....	43
2.2.3 Zero-Knowledge Proofs of Identity .....	44

2.2.4 Feige-Fiat Shamir Identification Scheme .....	46
<b>CHAPTER 3</b> <u>Multi-Prover Zero-Knowledge Proofs</u> .....	49
3.1 Introduction .....	50
3.2 Bit Commitment Schemes .....	50
3.2.1 Naor's Bit Commitment Scheme	
using Pseudo-Randomness .....	52
3.2.2 Naor's Scheme for Commit to Many Bits	
using Pseudo-Randomness .....	53
3.3 Multi-Prover Zero-Knowledge Interactive Proof Systems .....	54
3.3.1 The $k$ -Prover Model: Formal and Informal Definitions ..	54
3.3.2 Perfect Zero-Knowledge Proofs using 2-Prover	
for $NP$ languages .....	56
3.3.3 Efficient Identification Scheme using 2-Prover	
Interactive Proofs .....	63
<b>CHAPTER 4</b> <u>Interactive Proof Systems for <math>PSPACE</math> Languages</u> .....	66
4.1 Introduction .....	67
4.2 The Quantified Boolean Formula .....	67
4.3 The Arithmetization of Boolean Formulas .....	101
4.4 $PSPACE \subset IP$ .....	70
4.4.1 The Functional and The Randomized Form of	
An Arithmetic Form, $A$ .....	70
4.4.2 The Interactive Protocol for Proving that	
$A \neq 0 \pmod{p}$ .....	71
4.5 Interactive Proofs for $PSPACE$ Languages in One Round .....	73

## CHAPTER 5 A Zero-Knowledge Interactive Protocol for a Random

NP Language 76

5.1 Introduction ..... 76

5.2 Invulnerable Generators ..... 76

5.3 A Two-Envelope Zero-Knowledge Interactive Protocol  
for a Random Tiling Problem ..... 79

5.4 A Two-Prover Perfect Zero-Knowledge Interactive Protocol  
for a Random Tiling Problem in One Round ..... 88

5.5 Summary and Discussion ..... 89

REFERENCES ..... 91

ARABIC SUMMARY.

# **LIST OF ABBREVIATIONS**





## LIST OF ABBREVIATIONS

$AP$	The complexity class of average polynomial time problems.
$AM[q(n)]$	The class of languages recognized by an Arthur-Merlin game of $q(n)$ message exchanged.
$BCS$	Bit commitment scheme.
$BCS^*$	Bit commitment scheme without any intractability assumptions.
$B_i(s)$	The $i^{\text{th}}$ bit of a pseudo-random sequence on a seed $s$ .
$CoNP$	The class of problems whose complements are in $NP$ .
$CZK$	The class of languages which have computational zero-knowledge proofs.
$DTM$	Deterministic Turing machine.
$GI$	Graph isomorphism problem.
$GNP$	Graph nonisomorphism problem.
$G3C$	Graph 3-colourability.
$GMW$	Goldreich, Micali and Wigderson.
$G_j(s)$	The first $j$ bits of a pseudo-random sequence on a seed $s \in \{0, 1\}^n$ .
$IPS$	Interactive proof system.
$IP$	The class of languages which have interactive proofs.
$ITM$	Interactive Turing machine.
$MIP$	The class of languages which have multi-prover interactive proofs.
$M_1^*$	The simulator of $V^*$ .
$NP$	The class of languages recognizable by nondeterministic polynomial-time Turing machine.
$Pr((P, V) \text{ accepts } x)$	The probability that $(P, V)$ accepts the common input $x$ .
$PZK$	The class of languages which have perfect zero-knowledge proofs.
$(P, V)[x]$	The conversation space between $P$ and $V$ , on input $x$ .
$(P_1, \dots, P_k; V)$	$k$ -prover interactive protocol.

$PSPACE$	The class of all languages recognizable by polynomial space bounded $DTM$ programs that halts on all inputs.
$QRA$	Quadratic residuosity assumption.
$QBF$	Quantified Boolean formula problem.
$RNP$	The class of randomized decision problems.
$RTP$	Randomized Tiling problem.
$RSA$	Riverst, Shamir and Adleman.
$x \oplus y$	The bit by bit exclusive-or of bit strings $x$ and $y$ .
$x \in \{0, 1\}^n$	$x$ is a string of $n$ bits.
$SZK$	The class of languages which have statistical zero-knowledge proofs.
$Sym(N)$	The set of all possible permutations on $N$ where $N = \{1, 2, \dots, n\}$ .
$V$	Verifier.
$V^*$	Cheating verifier.
$V_P(x)$	$V$ 's output after interacting with $P$ on a common input $x$ .
$View_{(P^1, \dots, P_k, V)}(x)$	The verifier's view during the protocol.
$ZKIPS$	Zero-knowledge interactive proof systems.
$Z_p$	The set of integers $\{0, \dots, p-1\}$ , where $p$ is a prime. We can view $Z_p$ as a group with respect to addition modulo $p$ .
$Z_p^*$	The set of integers $\{z \in \{0, \dots, p-1\} : \gcd(z, p) = 1\}$ . We can view $Z_p^*$ as a group with respect to multiplication modulo $p$ .
$3SAT$	3-Satisfiability problem.
$\mu$	Probability distribution function.
$v(n)$	Any function vanishing faster than the inverse of any polynomial in $n$ .
$\Pi$	Decision problem.
$\{0, 1\}^n$	The set of all bit strings of length $n$ .
$l^n$	The concatenation of $n$ $l$ bits.

# **ACKNOWLEDGMENT**



## ACKNOWLEDGEMENT

*I would like to express my deepest gratitude and thankfulness to **Prof. Dr. Bayoumi Ibrahim Bayoumi**, Professor of Mathematics, Faculty of Science, Ain Shams University, for supervision, invaluable advices and comments and for his help during the preparation of the thesis.*

*I would like to express my deepest gratitude to **Dr. Mohamed Mahmod Mohamed Kouta**, Assistant Professor of Computer Science, Military Technical College, for suggesting the interesting point of research, kind supervision and offering unfailing support during the work.*

*I would like to express my deepest gratitude to **Dr. Fathy Saad Holail**, the Head of C. D. Division, Research Development Centre, National Defence Council, for his valuable guidance, helpful and useful discussions concerning this work.*

*I would like to express my deepest gratitude to **Prof. Dr. V. J. Rayward-Smith**, School of Information Systems, University of East Anglia, Norwich, United Kingdom. I owe him so much for his kind and sincere scientific supervision all through the year I spent in his lab.*

*Finally, to my **parents** and my **wife**.*

