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

بسم الله الرحمن الرحيم

CONTENTS

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^{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_{V^*}	The simulator of V^*.
NP	The class of languages recognizable by nondeterministic polynomial-time Turing machine.
$Pr((P, V)$ *accepts* $x)$	The probability that (P, V) accepts the common input x.
PZK	The class of languages which have perfect zero-knowledg proofs.
$(P, V)[x]$	The conversation space between P and V, on input x.
$(P_1, \ldots, P_k; V)$	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.
$View_{(P1, \dots, Pk, V)}(x)$	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.
μ	Probability distribution function.
$\nu(n)$	Any function vanishing faster than the inverse of any polynomial in n.
Π	Decision problem.
$\{0, 1\}^n$	The set of all bit strings of length n.
1^n	The concatenation of n 1 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.***