

TABLE OF CONTENTS

Chapter	Page No.
1. INTRODUCTION	1
1.1 Motivation	2
1.2 Related Work	3
1.3 Problem Statement	5
1.4 Scope of Work	7
1.5 Organization of Thesis	8
1.6 Conclusion	9
2. LITERATURE SURVEY	10
2.1 Objective	10
2.2 State Of Art	10
2.2.1 Wireless Sensor Networks	11
2.2.1.1 Design space of WSNs	12
2.2.1.2 Architecture & Node deployment in WSNs	13
2.2.1.3 Security Topology in WSNs	14
2.2.1.4 Security Perspective in Wireless Sensor Networks	15
2.2.1.5 Characteristics of a WSN	16
2.2.1.6 A Novel Group Key Agreement Protocol for WSN.....	17
2.2.1.7 Application of Timestamp Mechanism on WSNs	18
2.2.1.8 Dynamic Authentication in WSNs	18
2.2.2 Implementation Issues of Elliptic Curve Cryptography for WSN	19
2.2.3 One's complement for fast Scalar Multiplication in ECC for WSNs	19
2.3 Conclusion of Literature Survey	20
3. BASICS OF ECC	21
3.1 Mathematical Overview.....	21
3.1.1 Groups	21
3.1.2 Rings	21
3.1.3 Fields and Vector Spaces	22
3.1.4 Finite Fields.....	23
3.1.4.1 Prime Fields F_p	23
3.1.4.2 Binary Finite Field F_{2^m}	23

3.1.4.2.1 Polynomial Basis Representation of F_{2^m}	24
3.1.4.2.2 Normal Basis Representation of F_{2^m}	25
3.1.4.2.3 Gaussian Normal Bases.....	25
3.2 Elliptic Curves	26
3.2.1 Elliptic Curve Groups over Real Numbers	26
3.2.1.1 Elliptic Curve Addition: A Geometric Approach	27
3.2.1.1.1 Adding distinct points P & Q	27
3.2.1.1.2 Adding the points P & -P	28
3.2.1.1.3 Doubling the point P	29
3.2.1.1.4 Doubling the point P if $y_P=0$	30
3.2.1.2 Elliptic Curve Addition: An Algebraic Approach	31
3.2.1.2.1 Adding distinct points P & Q	31
3.2.1.2.2 Doubling the point P	31
3.2.2 Elliptic Curve Groups over F_p	31
3.2.2.1 Adding distinct points P & Q	32
3.2.2.2 Doubling the point P	33
3.2.3 Elliptic Curve Groups over F_{2^m}	33
3.2.3.1 Arithmetic in an Elliptic Curve Groups over F_{2^m}	33
3.2.3.1.1 Adding distinct points P & Q	34
3.2.3.1.2 Doubling the point P	34
3.3 Elliptic Curves Groups & Discrete Logarithm Problem	35
3.3.1 Elliptic Curve Discrete Logarithm Problem	35
3.4 Application of Elliptic Curves in Key Exchange	37
3.4.1 ECC domain parameters	37
3.4.2 Elliptic Curve Protocols	38
3.4.2.1 ECDH	39
3.4.2.2 ECDSA	40
3.4.2.3 ECAES	42
3.4.3 Algorithms for Elliptic Scalar Multiplication	43
3.4.3.1 Non adjacent form	44
3.4.4 Complexity Analysis of Elliptic Scalar Multiplication Algorithms...	45
3.4.4.1 Binary Method	45
3.4.4.2 Addition-Subtraction Method	46
3.4.4.3 Repeated Doubling Method	47
4. PROPOSED SCHEME	48
4.1 Introduction	48

4.2 Proposed Scheme	48
4.2.1 Notation Used	50
4.2.2 Diagrammatic Representation	53
4.2.3 Explanation of Proposed Scheme	60
5. SECURITY PERSPECTIVE & ANALYSIS OF PROPOSED SCHEME	66
5.1 Analysis of Attacks on Wireless Sensor Nodes	66
5.2 Analysis of General Attacks on any Participating Node	71
6. IMPLEMENTATION DETAILS & PERFORMANCE ANALYSIS	73
6.1 Implementation Details	73
6.2 Software Architecture of ECDSA	74
6.3 Class Structure of Implemented Modules	75
6.4 Results and Discussion.....	77
7. CONCLUSION	89
8. FUTURE WORK	90
9. REFERENCES AND BIBLIOGRAPHY	91
APPENDIX A	95