

Contents

List of Figures	xi
List of Tables	xiii
1 Introduction	1
1.1 Share a Secret with Multiple Parties	1
1.2 Scope of this Thesis	5
2 Basic Concepts	9
2.1 Components of a Secret Sharing Scheme	9
2.1.1 Participant Set and Access Structure	10
2.1.2 Distribution Function	12
2.1.3 Recreation Function	12
2.2 Some Access Structures and their Secret Sharing Schemes	13
2.2.1 Monotone Access Structures	13
2.2.2 Threshold Access Structures	14
2.2.3 Non-Monotone Access Structures	15
2.2.4 Non-Enclosing Access Structures	16
2.3 Realization of Secret Sharing Schemes	17
2.3.1 Simmons' Monotone Construction	17
2.3.2 Karnin's Lightweight Construction	18
2.3.3 Shamir's Threshold Scheme	18
2.4 Management Models and Operations	20
2.4.1 Management Model	20
2.4.2 Operations	20
2.5 Dynamic Secret Sharing	22
2.5.1 Disenrollment	24
2.5.2 Updating Access Structures	24
2.5.3 A Scheme with Disenrollment Capabilities	27
2.6 An Extension of the Concept of Management Models	30
2.6.1 A Third Phase in the Life Cycle of Secret Sharing Schemes	30
2.6.2 The Classical Model	31
2.6.3 Models for Dynamic Secret Sharing Schemes	32

2.7	Security in Secret Sharing	36
2.7.1	Perfectness	38
2.7.2	Robustness	44
2.8	Measures of Efficiency	50
2.9	Final Considerations	51
3	Access Structures and their Representation	53
3.1	Preliminaries	53
3.1.1	Notations	54
3.1.2	Data Structures	54
3.2	Identifying Non-Enclosing Access Structures	58
3.2.1	Representing Access Structures as Boolean Functions	58
3.2.2	Non-Enclosing Access Structures Given as Whitelists	60
3.3	Compositions of Monotone Substructures	64
3.3.1	Compositions of Threshold Substructures	65
3.3.2	Compositions of Monotone Substructures	67
3.4	Access Structures And Monotone Substructures	69
3.4.1	Identifying Monotone Substructures	69
3.4.2	Identifying Threshold Substructures	77
3.5	Final Considerations	82
4	Combiner Driven Management Models	85
4.1	Public Recreation and its Disadvantages	85
4.2	The Combiner as a Trusted Party	87
4.2.1	Combiner, Dealer and their Differences	87
4.2.2	Advantages of the Proposed Combiner	89
4.2.3	Disadvantages of the Proposed Combiner	91
4.3	The Combiner Driven Approach in Detail	92
4.3.1	Integrating the Combiner into the Entity Set	92
4.3.2	Management Models Using the Proposed Combiner	93
4.4	Perfectness and Efficiency Considerations	97
4.4.1	Robustness in Combiner Driven Schemes	97
4.4.2	Measures of Efficiency in Combiner Driven Schemes	99
4.5	Final Considerations	100
5	Fully Dynamic Combiner Driven Secret Sharing Schemes	101
5.1	A Scheme Realizing Threshold Access Structures	102
5.1.1	Adopting Shamir's Scheme	102
5.1.2	Construction	103
5.1.3	Recreation	104
5.1.4	General Updates of Threshold Access Structures	104
5.1.5	Numerical Aspects	108
5.1.6	Perfectness of the Combiner Driven Threshold Scheme	111

5.1.7	Robustness	114
5.1.8	Efficiency Considerations	120
5.1.9	Rating of the Scheme	122
5.2	A Scheme Realizing General Access Structures	123
5.2.1	Basic Idea of the Proposed Construction	124
5.2.2	Construction	125
5.2.3	Recreation	126
5.2.4	Exemplification of the Proposed Construction	127
5.2.5	General Updates of Arbitrary Access Structures	130
5.2.6	Additional features	134
5.2.7	Rating of the Scheme	135
5.3	Final Considerations	137
6	Secret Sharing Based on Error-Correcting Codes	139
6.1	Definitions for Error-Correcting Codes	139
6.2	Error-Correcting Codes and Secret Sharing	140
6.3	A New Construction for ECC-Based Schemes	141
6.3.1	Linked Access Structures	142
6.3.2	Generalization for Arbitrary Access Structures	147
6.3.3	Discussion of the Proposed Las-Vegas Algorithm	147
6.3.4	Choosing Non-Uniformly Distributed Masks	151
6.4	Deterministic Construction for Arbitrary Access Structures	154
6.4.1	Preliminaries	155
6.4.2	Example for Two Participants	156
6.4.3	On the Existence of Integral Solutions	159
6.4.4	Security Considerations	172
6.5	Final Considerations	175
7	Conclusions	177
7.1	Summary	177
7.2	Future Directions	178
	Bibliography	181