

Contents

1	Introduction	1
1.1	A Brief Review of Network Coding	1
1.2	Benefits of Network Coding	2
1.3	Applications of Network Coding	3
1.4	Insecurity of Network Coding	4
1.5	Book Organization	5
	References	5
2	Security Threats in Network Coding	9
2.1	Pollution Attack	9
2.1.1	Information-Theoretic Schemes	9
2.1.2	Cryptography-Based Schemes	10
2.2	Eavesdropping Attack	12
2.2.1	Shannon Security	12
2.2.2	Weak Security	13
2.2.3	Computational Security	14
2.3	Entropy Attack	15
2.4	Privacy Leakage	16
	References	17
3	Subspace Authentication for Random Linear Network Coding	21
3.1	Introduction	21
3.2	Problem Statement	23
3.2.1	Network Model	23
3.2.2	Adversary Model	24
3.3	Homomorphic Subspace Authentication	24
3.3.1	Basic Idea Overview	24
3.3.2	Homomorphic Subspace Signature	26
3.3.3	Batched Verification for HSS	27
3.3.4	Homomorphic Subspace MAC	28
3.3.5	Key Distribution for HSM	31

3.4	The MacSig Authentication Scheme	33
3.4.1	Tag Pollution	33
3.4.2	MacSig: Homomorphic MAC + Signature	34
3.4.3	Security Analysis of MacSig	36
3.5	Performance Evaluation	37
3.5.1	Bandwidth Overhead	37
3.5.2	Computation Overhead	38
3.6	Discussion	39
3.7	Conclusion	40
	References	40
4	Lightweight Encryption for Random Linear Network Coding	43
4.1	Introduction	43
4.2	Problem Statement	45
4.2.1	Network Model	45
4.2.2	Adversary Model	47
4.3	Security Analysis of Network Coding	48
4.4	P-Coding: The Proposed Scheme	51
4.4.1	Permutation Encryption	51
4.4.2	The P-Coding Scheme	52
4.4.3	The Enhanced P-Coding Scheme	53
4.5	Security Analysis	55
4.5.1	Probability Model	55
4.5.2	Attacks on P-Coding	57
4.5.3	Security of Enhanced P-Coding	60
4.6	Performance Evaluation	62
4.6.1	Analysis	62
4.6.2	Experiments	65
4.7	Discussion	67
4.8	Conclusion	67
	References	67
5	Anonymous Routing for Wireless Network Coding	69
5.1	Introduction	69
5.2	Problem Statement	71
5.2.1	System Model	71
5.2.2	Privacy Model	71
5.2.3	Adversary Model	73
5.3	ANOC: An Overview	73
5.3.1	Infeasibility of Onion Routing	74
5.3.2	Design Considerations of ANOC	75
5.4	ANOC: The Design Details	76
5.4.1	System Setup	76
5.4.2	Packet Format	77
5.4.3	Session Setup	78
5.4.4	Session Key Sharing	79

5.4.5	Auxiliary Decrypting	80
5.4.6	Session Teardown.....	81
5.5	Privacy Enhancement of ANOC.....	81
5.5.1	The External Adversary	81
5.5.2	The Internal Adversary	82
5.6	Performance Evaluation	84
5.7	Conclusion	90
	References	91
6	Concluding Remarks and Future Directions	95
6.1	Concluding Remarks.....	95
6.2	Future Directions.....	96
6.2.1	The Traceback Problem in Network Coding	96
6.2.2	Malicious Node Localization for Pollution Attacks.....	97
	References	97

Security in Network Coding

Zhang, P.; Lin, C.

2016, XI, 98 p. 34 illus., 18 illus. in color., Hardcover

ISBN: 978-3-319-31082-4