

# Contents

<b>A Study of Injection and Jamming Attacks in Wireless Secret Sharing Systems</b> . . . . .	1
Arsenia Chorti	
1 Introduction . . . . .	1
2 Secret Key Generation Systems in the Presence of an Active Adversary . . . . .	2
3 MiM in SKG Systems: Injection Attacks . . . . .	4
4 Jamming Attacks . . . . .	8
5 Conclusions . . . . .	12
References . . . . .	13
<b>Robust Secret Sharing for End-to-End Key Establishment with Physical Layer Keys Under Active Attacks.</b> . . . .	15
Stefan Pfennig, Sabrina Engelmann, Elke Franz and Anne Wolf	
1 Introduction . . . . .	15
2 System Model . . . . .	16
3 Physical Layer Key Generation . . . . .	19
4 End-to-End Key Establishment . . . . .	20
5 Conclusion . . . . .	31
References . . . . .	31
<b>Semantically-Secured Message-Key Trade-Off over Wiretap Channels with Random Parameters.</b> . . . .	33
Alexander Bunin, Ziv Goldfeld, Haim H. Permuter, Shlomo Shamai (Shitz), Paul Cuff and Pablo Piantanida	
1 Introduction . . . . .	34
2 Preliminaries . . . . .	37
3 SM-SK Trade-Off over Wiretap Channels with Non-Causal Encoder CSI . . . . .	38
4 Past Results as Special Cases . . . . .	42

5	Outline of Proof of Theorem 1	45
6	Summary and Concluding Remarks	46
	References	47
<b>Hash-then-Encode: A Modular Semantically Secure</b>		
	<b>Wiretap Code</b>	49
Setareh Sharifian, Fuchun Lin and Reihaneh Safavi-Naini		
1	Introduction	49
2	Preliminary	53
3	A Modular Construction of Efficiently Invertible UHF <sub>s</sub> (ei-UHF)	55
4	HtE (Hash-then-Encode) Construction	57
5	Concluding Remarks	61
	Appendix	62
	References	63
<b>A CCA-Secure Cryptosystem Using Massive MIMO Channels</b>		65
Thomas Dean and Andrea Goldsmith		
1	Introduction	65
2	System Model	67
3	Main Theorem	69
4	A CCA-Secure Cryptosystem	71
5	Conclusion	75
	References	76
<b>You Are How You Play: Authenticating Mobile Users via Game</b>		
<b>Playing</b>		79
Riccardo Spolaor, Merylin Monaro, Pasquale Capuozzo, Marco Baesso, Mauro Conti, Luciano Gamberini and Giuseppe Sartori		
1	Introduction	80
2	Related Work	81
3	Methods	83
4	Experimental Results	88
5	Conclusions	92
	References	94
<b>Fuzzy Authentication Using Rank Distance</b>		97
Alessandro Neri, Joachim Rosenthal and Davide Schipani		
1	Introduction	97
2	Rank Metric Codes and Linearized Polynomials	98
3	Fuzzy Commitment Scheme with the Rank Distance	100
4	A Linearized Polynomial Fuzzy Vault Scheme	101
5	Applications	107
	References	108

**A McEliece-Based Key Exchange Protocol for Optical Communication Systems** . . . . . 109

Joo Yeon Cho, Helmut Griesser and Danish Rafique

1 Introduction . . . . . 109

2 Background . . . . . 111

3 System Model . . . . . 113

4 A Proposed Key Exchange Protocol . . . . . 113

5 Security Analysis . . . . . 115

6 Implementation . . . . . 118

7 Conclusion . . . . . 120

Appendix . . . . . 120

References . . . . . 121

**An ICN-Based Authentication Protocol for a Simplified LTE Architecture** . . . . . 125

Alberto Compagno, Mauro Conti and Muhammad Hassan

1 Introduction . . . . . 125

2 ICN Overview . . . . . 127

3 Authentication and Mobile Management in LTE . . . . . 127

4 Simplified LTE Architecture for ICN . . . . . 130

5 Evaluation . . . . . 135

6 Security Discussion . . . . . 138

7 Conclusion . . . . . 139

References . . . . . 139

**Author Index** . . . . . 141

Proceedings of the 2nd Workshop on Communication  
Security

Cryptography and Physical Layer Security

Baldi, M.; Quaglia, E.A.; Tomasin, S. (Eds.)

2018, XIII, 141 p. 27 illus., 14 illus. in color., Hardcover

ISBN: 978-3-319-59264-0