

Contents

1	Physical Layer Security: A Paradigm Shift in Data Confidentiality	1
	Arsenia Chorti, Camilla Hollanti, Jean-Claude Belfiore and Harold Vincent Poor	
2	Secure Communication in Wiretap Channels with Partial and Statistical CSI at the Transmitter	17
	Eduard Jorswieck, Pin-Hsun Lin, Sabrina Engelmann and Anne Wolf	
3	MIMOME Gaussian Channels with GMM Signals in High-SNR Regime: Fundamental Limits and Tradeoffs	33
	Francesco Renna, Nicola Laurenti and Stefano Tomasin	
4	Performance Analysis of Transmission over AWGN Wiretap Channels with Practical Codes	53
	Marco Baldi, Franco Chiaraluce, Nicola Maturo and Stefano Tomasin	
5	Broadcast Channels with Confidential Messages: Channel Uncertainty, Robustness, and Continuity	69
	Rafael F. Schaefer, Andrea Grigorescu, Holger Boche and H. Vincent Poor	
6	End-to-End Key Establishment with Physical Layer Key Generation and Specific Attacker Models	93
	Stefan Pfennig, Elke Franz, Sabrina Engelmann and Anne Wolf	
7	Experimental Results on Secret-Key Extraction from Unsynchronized UWB Channel Observations	111
	Gianni Pasolini, Enrico Paolini, Davide Dardari and Marco Chiani	

8	Physical Layer Security in Power Line Communication Networks.	125
	Alberto Pittolo and Andrea M. Tonello	
9	Security Aspects of Compressed Sensing.	145
	Tiziano Bianchi and Enrico Magli	
10	Subspace Fuzzy Vault	163
	Kyle Marshall, Davide Schipani, Anna-Lena Trautmann and Joachim Rosenthal	
11	An Information Rate Improvement for a Polynomial Variant of the Naccache-Stern Knapsack Cryptosystem.	173
	Giacomo Micheli, Joachim Rosenthal and Reto Schnyder	
12	Implementation and Improvement of the Partial Sum Attack on 6-Round AES.	181
	Francesco Aldà, Riccardo Aragona, Lorenzo Nicolodi and Massimiliano Sala	
13	A Real Life Project in Cryptography: Assessment of RSA Keys	197
	Riccardo Aragona, Francesco Gozzini and Massimiliano Sala	
14	Encoding in the DTMF Channel for Two-Channel Authentication.	205
	Alessio Meneghetti, Pietro Peterlongo and Massimiliano Sala	

Physical and Data-Link Security Techniques for Future
Communication Systems

Baldi, M.; Tomasin, S. (Eds.)

2016, X, 212 p., Hardcover

ISBN: 978-3-319-23608-7