

# Contents

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

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



<http://www.springer.com/978-3-319-23608-7>

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