

# Contents

About the Special Issue Editor . . . . .	vii
Preface to "Side Channel Attacks" . . . . .	ix
<b>Seokhie Hong</b> Special Issue on "Side Channel Attacks" Reprinted from: <i>Appl. Sci.</i> <b>2019</b> , 9, 1881, doi:10.3390/app9091881 . . . . .	1
<b>Suhri Kim and Seokhie Hong</b> Single Trace Analysis on Constant Time CDT Sampler and Its Countermeasure Reprinted from: <i>Appl. Sci.</i> <b>2018</b> , 8, 1809, doi:10.3390/app8101809 . . . . .	6
<b>Soojung An, Suhri Kim, Sunghyun Jin, HanBit Kim, HeeSeok Kim</b> Single Trace Side Channel Analysis on NTRU Implementation Reprinted from: <i>Appl. Sci.</i> <b>2018</b> , 8, 2014, doi:10.3390/app8112014 . . . . .	22
<b>Sung Min Cho, Sunghyun Jin and HeeSeok Kim</b> Side-Channel Vulnerabilities of Unified Point Addition on Binary Huff Curve and Its Countermeasure Reprinted from: <i>Appl. Sci.</i> <b>2018</b> , 8, 2002, doi:10.3390/app8102002 . . . . .	39
<b>Yoo-Seung Won, Jonghyeok Lee and Dong-Guk Han</b> Side Channel Leakages Against Financial IC Card of the Republic of Korea † Reprinted from: <i>Appl. Sci.</i> <b>2018</b> , 8, 2258, doi:10.3390/app8112258 . . . . .	62
<b>Bo-Yeon Sim, Junki Kang and Dong-Guk Han</b> Key Bit-Dependent Side-Channel Attacks on Protected Binary Scalar Multiplication † Reprinted from: <i>Appl. Sci.</i> <b>2018</b> , 8, 2168, doi:10.3390/app8112168 . . . . .	79
<b>Samira Briongos, Pedro Malagón, Juan-Mariano de Goyeneche and Jose M. Moya</b> Cache Misses and the Recovery of the Full AES 256 Key Reprinted from: <i>Appl. Sci.</i> <b>2019</b> , 9, 944, doi:10.3390/app9050944 . . . . .	99
<b>Youngjoo Shin</b> Fast and Secure Implementation of Modular Exponentiation for Mitigating Fine-Grained Cache Attacks Reprinted from: <i>Appl. Sci.</i> <b>2018</b> , 8, 1304, doi:10.3390/app8081304 . . . . .	123
<b>Krzysztof Gołofit and Piotr Z. Wiczorek</b> Chaos-Based Physical Unclonable Functions Reprinted from: <i>Appl. Sci.</i> <b>2019</b> , 9, 991, doi:10.3390/app9050991 . . . . .	133
<b>Yuichi Komano and Shoichi Hirose</b> Re-Keying Scheme Revisited: Security Model and Instantiations Reprinted from: <i>Appl. Sci.</i> <b>2019</b> , 9, 1002, doi:10.3390/app9051002 . . . . .	150
<b>Naila Mukhtar, Mohamad Ali Mehrabi, Yinan Kong and Ashiq Anjum</b> Machine-Learning-Based Side-Channel Evaluation of Elliptic-Curve Cryptographic FPGA Processor Reprinted from: <i>Appl. Sci.</i> <b>2019</b> , 9, 64, doi:10.3390/app9010064 . . . . .	165

<b>Dongyoung Koo, Youngjoo Shin, Joobeom Yun and Junbeom Hur</b> Improving Security and Reliability in Merkle Tree-Based Online Data Authentication with Leakage Resilience Reprinted from: <i>Appl. Sci.</i> <b>2018</b> , <i>8</i> , 2532, doi:10.3390/app8122532 . . . . .	<b>185</b>
<b>Yang Li, Momoka Kasuya and Kazuo Sakiyama</b> Comprehensive Evaluation on an ID-Based Side-Channel Authentication with FPGA-Based AES Reprinted from: <i>Appl. Sci.</i> <b>2018</b> , <i>8</i> , 1898, doi:10.3390/app8101898 . . . . .	<b>214</b>
<b>Ming-Yang Su, Hong-Siou Wei, Xin-Yu Chen, Po-Wei Lin and Ding-You Qiu</b> Using Ad-Related Network Behavior to Distinguish Ad Libraries Reprinted from: <i>Appl. Sci.</i> <b>2018</b> , <i>8</i> , 1852, doi:10.3390/app8101852 . . . . .	<b>228</b>