

# Nicholas Kolokotronis

## Curriculum vitae

Univ. Peloponnese  
Dept. Informatics and Telecomm  
☎ (+30) 2710 372231  
✉ [nkolok@uop.gr](mailto:nkolok@uop.gr)  
🌐 [www.uop.gr/~nkolok](http://www.uop.gr/~nkolok)

June 2017

### Personal details

#### Education

- 1998–2003 **Ph.D. in Cryptography**  
University of Athens, Department of Informatics and Telecommunications  
*Thesis:* Nonlinear signal processing and applications to cryptography
- 1996–1998 **M.Sc. in Computer Science**  
University of Athens, Department of Informatics and Telecommunications  
*Specialization:* High Performance Algorithms  
*Grade:* 8,55/10  
*Thesis:* Image compression, progressive transmission, and selective decompression by using wavelets
- 1990–1995 **B.Sc. in Mathematics**  
Aristotle University of Thessaloniki, Department of Mathematics  
*Specialization:* Applied Mathematics  
*Grade:* 7,85/10

#### Awards

- 1994 Hellenic State Scholarship's Foundation (IKY) award for performance excellence during the third academic year of undergraduate studies

### Positions held

#### Main position

- 2012–today **Assistant professor**  
University of Peloponnese, Department of Informatics and Telecommunications
- 2008–2012 **Lecturer**  
University of Peloponnese, Department of Informatics and Telecommunications
- 2004–2008 **Adjunct faculty**  
University of Peloponnese, Department of Informatics and Telecommunications

#### Other positions

- 2015–today **Visiting instructor**  
Open University of Cyprus, Faculty of Pure and Applied Sciences
- 2005–today **Adjunct faculty**  
University of Athens, Department of Informatics and Telecommunications
- 2004–2006 **Adjunct faculty**  
University of Piraeus, Department of Digital Systems

- 2002–2004 **IT consultant**  
European Dynamics SA, e–Business Division
- 2001–2002 **Software engineer**  
Hellenic Armed Forces, Research and Informatics Corps
- 1998–2001 **Research assistant**  
University of Athens, Department of Informatics and Telecommunications

## Research interests

- **Applied cryptography:** block/stream ciphers and pseudorandom generators, s–box design, boolean functions, statistical cryptanalysis, blockchain
- **Modern cryptography:** weak and strong pseudorandom functions (PRFs), semantic security, cryptographic applications of statistical learning (LPN, LWE, etc.), game–theoretic cryptography
- **Post–quantum cryptography:** code–based cryptosystems, general decoding attacks (ISD), lattice–based cryptosystems, quantum algorithms
- **Information security:** statistical database security, anonymity protocols and systems, biometric security, multimedia security
- **Cyber–security:** IoT security, network security protocols, wireless security, security in M2M communications
- **PHY layer security:** information–theoretic security, cooperative protocols (DF, AF, CJ), game–theoretic security, partner selection schemes
- **Trust management:** trust models, reputation management, game theory and trust, information–theoretic trust notions
- **Error correcting codes:** random codes, probabilistic (list) decoding and complexity issues, codes for the wiretap channel, joint error correction and encryption

## Teaching experience

### Postgraduate

- |            |  |                          |
|------------|--|--------------------------|
| 2015–today | Computer and network security: advanced topics (co–instructor) | <i>Univ. Cyprus</i>      |
| 2013–2015  | Topics in cryptographic algorithms design                      | <i>Univ. Peloponnese</i> |
| 2013–2015  | Topics in communications security                              | <i>Univ. Peloponnese</i> |
| 2009–2011  | Cryptography and applications                                  | <i>Univ. Peloponnese</i> |
| 2009–2011  | Information theory and coding                                  | <i>Univ. Peloponnese</i> |
| 2005–today | Systems security (co–instructor)                               | <i>Univ. Athens</i>      |
| 2005       | Networked systems security                                     | <i>Univ. Piraeus</i>     |
| 1998–2000  | Information theory and coding (co–instructor)                  | <i>Univ. Athens</i>      |

### Undergraduate

- |            |  |                          |
|------------|--|--------------------------|
| 2015       | Mathematics II (co–instructor)                   | <i>Univ. Peloponnese</i> |
| 2013–today | Probability and statistics (co–instructor)       | <i>Univ. Peloponnese</i> |
| 2012–2013  | Linear algebra and number theory (co–instructor) | <i>Univ. Peloponnese</i> |
| 2009–2013  | Information theory and coding                    | <i>Univ. Peloponnese</i> |
| 2007–2008  | Introduction to programming                      | <i>Univ. Peloponnese</i> |
| 2006       | Advanced cryptography                            | <i>Univ. Peloponnese</i> |

2005	Number theory	<i>Univ. Peloponnese</i>
2004–today	Cryptography	<i>Univ. Peloponnese</i>
2004–today	Systems security	<i>Univ. Peloponnese</i>
2004–2005	Information security	<i>Univ. Piraeus</i>
2004	Signals and systems	<i>Univ. Piraeus</i>
1998–2000	Digital signal processing (co–instructor)	<i>Univ. Athens</i>

## Supervision of students

### Doctoral

2015	P. Smyrli, Post–quantum cryptography: code–based cryptosystems	<i>ongoing</i>
2013	K. Ntemos, Stochastic games, cognitive radio networks, and security (co–supervisor)	<i>ongoing</i>
2007	K. Limniotis, Cryptographically–related complexity measures for binary sequences (co–supervisor)	<i>completed</i>

### Postgraduate

2016	I. Lytsiou, Cryptocurrencies: models, security, and applications	<i>completed</i>
2016	I. Galanos, Social networks and personal data protection	<i>completed</i>
2015	C. Karzis, Formal security models in symmetric cryptosystems	<i>completed</i>
2015	S. Brotsis, Hard problems with applications in the design of public–key cryptosystems	<i>completed</i>
2015	I. Christakis, Man–in–the–middle attacks in SSL/TLS network security protocols	<i>completed</i>
2014	M. Athanasakos, Security of wireless communications against passive attacks at the physical layer	<i>completed</i>
2014	P. Smyrli, Code–based cryptosystems: constructions and attacks	<i>completed</i>
2014	N. Charitos, Security at the internet of things	<i>completed</i>
2013	J. Faklaris, Smart grid security	<i>completed</i>
2013	T. Mouratis, Secure electronic mail services in iOS platform	<i>completed</i>
2012	Z. Dermatis, Secure routing in wireless mobile networks	<i>completed</i>
2012	M. Droulia, Cognitive radio network security	<i>completed</i>
2011	A. Schizas, Cryptanalytic attacks on the RSA algorithm	<i>completed</i>
2010	E. Bozis, Security analysis and implementation issues of authentication protocols	<i>completed</i>

### Undergraduate

2016	D. Mentesidis, Wireless communication technologies for public safety	<i>completed</i>
2015	G. Panagopoulos, Trust management models in P2P networks	<i>ongoing</i>
2015	G. Geramanis, Attacks on anonymity services and protocols	<i>ongoing</i>
2014	S. Magklaris, Poodle and related attacks on SSL/TLS security protocols	<i>completed</i>
2011	V. Vlahogianni, Security/authentication issues in RFID tags	<i>completed</i>
2010	G. Gogolis, Analysis and implementation of RBAC security model (co–supervisor)	<i>completed</i>
2009	K. Psarakis, Services and security in e–banking systems	<i>completed</i>
2008	M. Grimani, Analysis of cryptographic characteristics in contemporary	<i>completed</i>

	stream ciphers	
2007	E. Aggelis, Security analysis of the new version of the IPsec protocol	<i>completed</i>
2006	M. Anthi and E. Kasimati, Turbo codes and interleavers based on permutation polynomials (co-supervisor)	<i>completed</i>
2005	D.-R. Koukoutsaki and D.-E. Reggli, Overview of modern cryptographic and cryptanalytic techniques (co-supervisor)	<i>completed</i>

## Committees, working groups

### Administrative positions

2015–2016	Member of the undergraduate studies program committee	<i>Dept. IT</i>
2013–2015	Member of the NSRF project “information system development for the quality assurance unit at the University of Peloponnese”	<i>Univ. Peloponnese</i>
2012–2013	Member of the undergraduate studies program committee	<i>Dept. IT</i>
2011–today	Member of evaluation committees for the procurement of goods	<i>Univ. Peloponnese</i>
2010–2016	Department’s leader in the NSRF project “higher education training at the University of Peloponnese”	<i>Univ. Peloponnese</i>
2009–2016	Member of the development and maintenance team of the website <a href="http://dit.uop.gr">dit.uop.gr</a>	<i>Dept. IT</i>
2008–today	Member of the <i>algorithms, cryptography and computational logic</i> laboratory	<i>Dept. IT</i>
2008–today	Member of the department’s General Assembly as well as Special General Assembly	<i>Dept. IT</i>

### Evaluation committees

2005–2007	Member of external evaluation committee for tenders submitted to the General Secretariat of Commerce (GSC), Ministry of Development
2004–2005	Regular evaluator of research projects and proposals submitted to the General Secretariat for Research and Technology (GSRT)

### Expert working groups

2000–2002	Member of working groups for the professional training of the National Committee of Telecommunications and Posts (NCTP) staff on issues of telecommunication networks security
-----------	--

### Other memberships

1998–today	Member of the IEEE (computer and IT societies)
------------	--

## Academic service

Editor	<ul style="list-style-type: none"> <li>○ <b>AE:</b> EURASIP J. Wireless Commun. Netw.</li> </ul>	<i>2009–2017</i>
Reviewer	<ul style="list-style-type: none"> <li style="width: 50%;">○ Adv. Math. Commun.</li> <li style="width: 50%;">○ IEEE Trans. Inf. Theory</li> <li style="width: 50%;">○ Appl. Algebra Engrg. Comm. Comput.</li> <li style="width: 50%;">○ IEEE Trans. Multimedia</li> <li style="width: 50%;">○ Benchmarking Int. J.</li> <li style="width: 50%;">○ IEEE Trans. Vehicular Tech.</li> <li style="width: 50%;">○ Comput. Standards Interfaces</li> <li style="width: 50%;">○ Inform. Comput. Security</li> <li style="width: 50%;">○ Cryptogr. Commun.</li> <li style="width: 50%;">○ Inform. Process. Lett.</li> <li style="width: 50%;">○ Des. Codes Cryptogr.</li> <li style="width: 50%;">○ Int. J. Comput. Math.</li> </ul>	

- Discrete Appl. Math.
- Discrete Math.
- EURASIP J. Wireless Commun. Netw.
- Finite Fields Appl.
- IEEE Commun. Lett.
- IEEE Trans. Commun.
- IEEE Trans. Inf. Forensics & Security
- Int. J. Electron. Governance
- J. Complexity
- J. Comput. Sci. Tech.
- J. Signal Image Video Process.
- Security Commun. Netw.
- Signal Process.

TPC member	<ul style="list-style-type: none"> <li>○ E-DEM (Conf. e-Democracy Security Priv. Trust)</li> <li>○ DSP (Int. Conf. Digit. Signal Process.)</li> <li>○ EUSIPCO (Eur. Signal Process. Conf.)</li> <li>○ ICASSP (Int. Conf. Acoust. Speech Signal Process.)</li> <li>○ ICCS (Int. Conf. Comput. Sci.)</li> <li>○ IEEE GLOBECOM (Commun. Inf. Security Symp.)</li> <li>○ IEEE ICC (Int. Conf. Commun.)</li> <li>○ IEEE ISCAS (Int. Symp. Circuits Syst.)</li> <li>○ IEEE ISIT (Int. Symp. Inf. Theory)</li> <li>○ IEEE MELECON (Mediterranean Electrotech. Conf.)</li> <li>○ IEEE WDFIA (Wkshp Digit. Forensics Incident Anal.)</li> <li>○ ISPEC (Inform. Security Pract. Experience Conf.)</li> <li>○ MCIS (Mediterranean Conf. Inf. Syst.)</li> <li>○ PARA (Wkshp SoA Sci. Parallel Comput.)</li> <li>○ PCI (Panhellenic Conf. Inform.)</li> </ul>	<p>2013, 2015, 2017</p> <p>2009, 2011</p> <p>1998, 2008</p> <p>2012</p> <p>2006–2007</p> <p>2009</p> <p>2011</p> <p>2003</p> <p>2003, 2011, 2013, 2015</p> <p>2016</p> <p>2007–2010</p> <p>2014</p> <p>2009</p> <p>2006</p> <p>2010</p>
------------	--	---

## Projects, grants

### Grants

- |           |  |  |
|-----------|--|--|
| 2006–2008 | <p>Study of complexity and pseudorandomness properties in symmetric encryption algorithms</p> <p><i>Coordinator:</i> University of Athens</p> <p><i>Funding:</i> British Council</p> | <p><i>Grant:</i> 70/3/8470</p> <p><i>Budget:</i> 16,0 K€</p> |
| 2005      | <p>Study of stream ciphers in symmetric cryptography</p> <p><i>Coordinator:</i> University of Athens</p> <p><i>Funding:</i> University of Athens</p>                                 | <p><i>Grant:</i> 70/4/7818</p> <p><i>Budget:</i> 4,5 K€</p>  |

### Research projects

- |           |  |  |
|-----------|--|--|
| 2013–2016 | <p>HANDICAMS: heterogeneous ad-hoc networks for distributed, cooperative, and adaptive multimedia signal processing</p> <p><i>Coordinator:</i> Katholieke Univ. Leuven</p> <p><i>Funding:</i> European Commission, FP7</p> | <p><i>Grant:</i> FET-323944</p> <p><i>Budget:</i> 2,0 M€</p>   |
| 2012–2015 | <p>ART-IN-SPACE: adaptive, robust to threats, immune to nonlinearities, sparse opportunistic cognitive radio</p> <p><i>Coordinator:</i> University of Athens</p> <p><i>Funding:</i> NSRF Excellence Program</p>            | <p><i>Grant:</i> 70/3/11918</p> <p><i>Budget:</i> 157,5 K€</p> |

- 2012–2015 SWINCOM: secure wireless nonlinear communications at the physical layer  
*Coordinator:* University of Athens *Grant:* 70/3/11668  
*Funding:* NSRF Thalys Program *Budget:* 512,8 K€
- 2004–2007 ECON–TISP: application of economic theories to design and develop telecommunications and information systems and products  
*Coordinator:* University of Athens *Grant:* 56/90/7425  
*Funding:* Community Support Frwk III *Budget:* 90,0 K€
- 2004–2007 SECURE–JUSTICE: secure communication and collaboration framework for the judicial cooperation environment  
*Coordinator:* Project Automation SpA *Grant:* IST-2002-507188  
*Funding:* European Commission, FP6 *Budget:* 5,4 M€
- 2002–2005 DIASTASIS: digital era statistical indicators – definition, measurement and exploitation of new socio-economic indicators correlating web usage statistical data and household research  
*Coordinator:* European Dynamics SA *Grant:* IST-2000-31083  
*Funding:* European Commission, FP5 *Budget:* 2,0 M€
- 2002–2005 ICTE–PAN: methodologies and tools for building intelligent collaboration and transaction environments in public administration networks  
*Coordinator:* European Dynamics SA *Grant:* IST-2001-35120  
*Funding:* European Commission, FP5 *Budget:* 3,2 M€
- 2000–2001 CHANNEL SOUNDER: development of an intelligent measurement device for the multidimensional characterization of broadband radio channels  
*Coordinator:* Nat. Tech. Univ. Athens *Grant:* 61/1189  
*Funding:* General Secretariat R&T *Budget:* 176,1 K€
- 1999–2001 BILLING MALL: development of an integrated e–commerce platform for secure billing management in subscription services  
*Coordinator:* University of Athens *Grant:* 70/3/4483  
*Funding:* General Secretariat R&T *Budget:* 1,1 M€
- 1996–1998 EUROMED: technologies for founding of a european telemedical information society  
*Coordinator:* Nat. Tech. Univ. Athens *Grant:* 70/3/2723  
*Funding:* European Commission, TEDIS *Budget:* 1,6 M€

### Consulting projects

- 2007 Technical action plan and specifications of supplementary technical infrastructures for operating the General Business Register (GBR)  
*Coordinator:* University of Athens *Grant:* 70/3/9291  
*Funding:* General Secretariat Comm. *Budget:* –
- 2000 Consulting services for supporting the Public Power Corporation (PPC) enter the telecommunications market  
*Coordinator:* University of Athens *Grant:* 70/3/5328  
*Funding:* Public Power Corporation *Budget:* –
- 2000 Public consultation and tender documents of individual licenses for the provisioning of mobile communication, fixed wireless access, and DECT services  
*Coordinator:* University of Athens *Grant:* 70/3/5255  
*Funding:* Nat. Comm. Telecomm. Posts *Budget:* –
- 1999 Development of telecommunications security policies  
*Coordinator:* University of Athens *Grant:* 70/3/4706  
*Funding:* Ministry Transp. Telecomm. *Budget:* –

## Research activities

### Invited talks

- Cryptographic Boolean functions with maximum algebraic immunity. *2016 International Conference on Cryptography, Cyber–Security, and Information Warfare*, May 2016, Athens, Greece
- On the computation of best second–order approximations of boolean functions. *2014 International Conference on Cryptography, Network Security and Applications in Armed Forces*, Apr. 2014, Athens, Greece
- Code–based public–key cryptosystems: constructions and attacks. *2014 Athens Cryptography Day (ATHECRYPT)*, Jan. 2014, Athens, Greece
- Cryptanalytic attacks and related criteria for stream and block ciphers. *2011 Intensive Program on Information Communication Security (IPICS)*, Aug. 2011, Corfu, Greece
- Towards computing best quadratic approximations. *Information Security Group, Royal Holloway University of London*, Dec. 2006, Surrey, U.K.
- E–commerce security. *National Committee of Telecommunications and Posts*, Nov. 2002, Athens, Greece
- Analysis and design of symmetric cryptographic algorithms. *2001 National Conference on Cyberspace Security and Hacking*, Oct. 2001, Athens, Greece
- Telecommunications security. *National Committee of Telecommunications and Posts*, Apr. 2000, Athens, Greece

### Schools, seminars

- Topics in cryptographic design and cryptanalysis. *ECRYPT Summer School*, May 2007, Samos, Greece

## Publications

### Books, edited volumes

- [1] N. Kolokotronis and C. D. Koutras, “Zero knowledge proofs and applications,” in *Modern Cryptography: Theory and Applications*, M. Burmester, S. Gritzalis, S. K. Katsikas, and V. Chrissikopoulos, Eds. Papatotiriou Pubs, 2011, pp. 635–646. [[online](#)]
- [2] N. Kolokotronis, “Stream ciphers,” in *Modern Cryptography: Theory and Applications*, M. Burmester, S. Gritzalis, S. K. Katsikas, and V. Chrissikopoulos, Eds. Papatotiriou Pubs, 2011, pp. 299–354. [[online](#)]
- [3] N. Kolokotronis and K. Limniotis, “Algorithmic algebra,” in *Modern Cryptography: Theory and Applications*, M. Burmester, S. Gritzalis, S. K. Katsikas, and V. Chrissikopoulos, Eds. Papatotiriou Pubs, 2011, pp. 47–87. [[online](#)]
- [4] N. Kolokotronis and C. D. Koutras, “Anonymity measures and privacy preservation techniques,” in *Protecting Privacy in Information and Communication Technologies: Technical and Legal Issues*, C. Lambrinouidakis, L. Mitrou, S. Gritzalis, and S. K. Katsikas, Eds. Papatotiriou Pubs, 2010, pp. 123–145. [[online](#)]
- [5] P. Kanellis, E. Kiountouzis, N. Kolokotronis, and D. Martakos, *Digital crime and forensic science in cyberspace*. IGI Global Publishing, April 2006. [[online](#)]
- [6] N. Kolokotronis, “Nonlinear signal processing and applications to cryptography,” Ph.D Thesis, Department of Informatics and Telecommunications, National and Kapodistrian University of Athens, December 2003. [[online](#)]



- [7] E. Kofidis, N. Kolokotronis, A. Vassilarakou, S. Theodoridis, and D. Cavouras, "Medical image compression," in *Advanced Infrastructures for Future Healthcare*, Studies in Health Technology and Informatics, A. Marsh, L. Grandinetti, and T. Kauranne, Eds. IOS Press, 2000, vol. 79, pp. 369–406. [[online](#)]

### Journals

- [8] K. Limniotis and N. Kolokotronis, "Boolean functions with maximum algebraic immunity: further extensions of the Carlet–Feng construction," *Designs, Codes and Cryptography*, 2017, accepted (minor comments).
- [9] N. Kolokotronis, A. Katsiotis, and N. Kalouptsidis, "Secretly pruned convolutional codes: security analysis and performance results," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 7, pp. 1500–1514, July 2016. [[online](#)]
- [10] K. Limniotis, N. Kolokotronis, and N. Kalouptsidis, "Secondary constructions of boolean functions with maximum algebraic immunity," *Cryptography and Communications*, vol. 5, no. 3, pp. 179–199, September 2013. [[online](#)]
- [11] N. Kolokotronis, K. Limniotis, and N. Kalouptsidis, "Best affine and quadratic approximations of particular classes of boolean functions," *IEEE Transactions on Information Theory*, vol. 55, no. 11, pp. 5211–5222, November 2009. [[online](#)]
- [12] T. Etzion, N. Kalouptsidis, N. Kolokotronis, K. Limniotis, and K. G. Paterson, "Properties of the error linear complexity spectrum," *IEEE Transactions on Information Theory*, vol. 55, no. 10, pp. 4681–4686, October 2009. [[online](#)]
- [13] N. Kolokotronis, K. Limniotis, and N. Kalouptsidis, "Factorization of determinants over finite fields and application in stream ciphers," *Cryptography and Communications*, vol. 1, no. 2, pp. 135–165, July 2009. [[online](#)]
- [14] K. Limniotis, N. Kolokotronis, and N. Kalouptsidis, "On the linear complexity of sequences obtained by state space generators," *IEEE Transactions on Information Theory*, vol. 54, no. 4, pp. 1786–1793, April 2008. [[online](#)]
- [15] N. Kolokotronis, "Cryptographic properties of nonlinear pseudorandom number generators," *Designs, Codes and Cryptography*, vol. 46, no. 3, pp. 353–363, March 2008. [[online](#)]
- [16] K. Limniotis, N. Kolokotronis, and N. Kalouptsidis, "On the nonlinear complexity and Lempel–Ziv complexity of finite length sequences," *IEEE Transactions on Information Theory*, vol. 53, no. 11, pp. 4293–4302, November 2007. [[online](#)]
- [17] P. Rizomiliotis, N. Kolokotronis, and N. Kalouptsidis, "On the quadratic span of binary sequences," *IEEE Transactions on Information Theory*, vol. 51, no. 5, pp. 1840–1848, May 2005. [[online](#)]
- [18] N. Kolokotronis, G. Gatt, and N. Kalouptsidis, "On the generation of sequences simulating higher order white noise for system identification," *Signal Processing*, vol. 84, no. 5, pp. 833–852, May 2004. [[online](#)]
- [19] N. Kolokotronis and N. Kalouptsidis, "On the linear complexity of nonlinearly filtered PN-sequences," *IEEE Transactions on Information Theory*, vol. 49, no. 11, pp. 3047–3059, November 2003. [[online](#)]



- [20] N. Kolokotronis, P. Rizomiliotis, and N. Kalouptsidis, "Minimum linear span approximation of binary sequences," *IEEE Transactions on Information Theory*, vol. 48, no. 10, pp. 2758–2764, October 2002. [[online](#)]
- [21] C. Margaritis, N. Kolokotronis, P. Papadopoulou, D. Martakos, and P. Kanellis, "Securing web-based information systems: a model and implementation guidelines," *Informatica (Slovenia)*, vol. 26, no. 2, pp. 159–168, July 2002, Special issue: security and protection. [[online](#)]
- [22] N. Kolokotronis, C. Margaritis, P. Papadopoulou, P. Kanellis, and D. Martakos, "An integrated approach for securing electronic transactions over the web," *Benchmarking: An International Journal*, vol. 9, no. 2, pp. 166–181, March 2002, Special issue: electronic commerce – a best practice perspective. [[online](#)]
- [23] E. Kofidis, N. Kolokotronis, A. Vassilarakou, S. Theodoridis, and D. Cavouras, "Wavelet-based medical image compression," *Future Generation Computer Systems*, vol. 15, no. 2, pp. 223–243, March 1999. [[online](#)]

#### Conferences (refereed)

- [24] K. Ntemos, N. Kalouptsidis, and N. Kolokotronis, "Trust-based strategies for wireless networks under partial monitoring," in *25th European Signal Processing Conference – EUSIPCO*. EURASIP, August 2017, accepted.
- [25] K. Ntemos, N. Kolokotronis, and N. Kalouptsidis, "Using trust to mitigate malicious and selfish behavior of autonomous agents in CRNs," in *27th IEEE Annual International Symposium on Personal, Indoor, and Mobile Radio Communications – PIMRC*, September 2016, pp. 1–7. [[online](#)]
- [26] N. Kolokotronis and M. Athanasakos, "Improving physical layer security in DF relay networks via two-stage cooperative jamming," in *24rd European Signal Processing Conference – EUSIPCO*. EURASIP, August 2016, pp. 1173–1177. [[online](#)]
- [27] K. Limniotis and N. Kolokotronis, "Boolean functions with maximum algebraic immunity based on properties of punctured Reed–Muller codes," in *2nd International Conference on Cryptography and Information Security in the Balkans – BALKANCRYPTSEC*, Lecture Notes in Computer Science, E. Pasalic and L. R. Knudsen, Eds., vol. 9540. Berlin, Germany: Springer, September 2015, pp. 3–16. [[online](#)]
- [28] K. Ntemos, N. Kalouptsidis, and N. Kolokotronis, "Managing trust in diffusion adaptive networks with malicious agents," in *23rd European Signal Processing Conference – EUSIPCO*. EURASIP, August 2015, pp. 91–95. [[online](#)]
- [29] A. Katsiotis, N. Kolokotronis, and N. Kalouptsidis, "Secure encoder designs based on turbo codes," in *2015 IEEE International Conference on Communications – ICC*, June 2015, pp. 4315–4320. [[online](#)]
- [30] N. Kolokotronis, K. Fytrakis, A. Katsiotis, and N. Kalouptsidis, "A cooperative jamming protocol for physical layer security in wireless networks," in *2015 IEEE International Conference on Acoustics, Speech and Signal Processing – ICASSP*, April 2015, pp. 5803–5807. [[online](#)]
- [31] N. Kolokotronis, K. Fytrakis, A. Katsiotis, and N. Kalouptsidis, "Cooperation for secure wireless communications with resource-bounded eavesdroppers," in *2014 IEEE Global Communications Conference – GLOBECOM, Workshop on Trusted Communications with Physical Layer Security (TPLS)*, December 2014, pp. 1483–1488. [[online](#)]

- [32] N. Kolokotronis, A. Katsiotis, and N. Kalouptsidis, "Attacking and defending lightweight PHY security schemes for wireless communications," in *7th ACM Conference on Security and Privacy in Wireless and Mobile Networks – WISEC*, July 2014, pp. 177–182. [[online](#)]
- [33] A. Katsiotis, N. Kolokotronis, and N. Kalouptsidis, "Physical layer security via secret trellis pruning," in *24th IEEE Annual International Symposium on Personal, Indoor, and Mobile Radio Communications – PIMRC*, September 2013, pp. 507–512. [[online](#)]
- [34] N. Kolokotronis and K. Limniotis, "A greedy algorithm for checking normality of cryptographic boolean functions," in *International Symposium on Information Theory and its Applications – ISITA*. IEEE, October 2012, pp. 601–605. [[online](#)]
- [35] N. Kolokotronis and K. Limniotis, "On the second-order nonlinearity of cubic Maiorana–McFarland boolean functions," in *International Symposium on Information Theory and its Applications – ISITA*. IEEE, October 2012, pp. 596–600. [[online](#)]
- [36] K. Limniotis, N. Kolokotronis, and N. Kalouptsidis, "Constructing boolean functions in odd number of variables with maximum algebraic immunity," in *2011 IEEE International Symposium on Information Theory – ISIT*, July 2011, pp. 2686–2690. [[online](#)]
- [37] N. Kalouptsidis and N. Kolokotronis, "Fast decoding of regular LDPC codes using greedy approximation algorithms," in *2011 IEEE International Symposium on Information Theory Proceedings – ISIT*, July 2011, pp. 2005–2009. [[online](#)]
- [38] T. Etzion, N. Kalouptsidis, N. Kolokotronis, K. Limniotis, and K. G. Paterson, "On the error linear complexity profiles of binary sequences of period  $2^n$ ," in *2008 IEEE International Symposium on Information Theory – ISIT*, July 2008, pp. 2400–2404. [[online](#)]
- [39] N. Kolokotronis, "On symplectic matrices of cubic boolean forms and connections with second order nonlinearity," in *2008 IEEE International Symposium on Information Theory – ISIT*, July 2008, pp. 1636–1640. [[online](#)]
- [40] N. Kolokotronis, K. Limniotis, and N. Kalouptsidis, "Efficient computation of the best quadratic approximations of cubic boolean functions," in *11th IMA Conference on Cryptography and Coding – IMACC*, Lecture Notes in Computer Science, S. D. Galbraith, Ed., vol. 4887. Berlin, Germany: Springer, December 2007, pp. 73–91. [[online](#)]
- [41] N. Kolokotronis, K. Limniotis, and N. Kalouptsidis, "Improved bounds on the linear complexity of keystreams obtained by filter generators," in *2007 Information Security and Cryptology – INSCRYPT*, Lecture Notes in Computer Science, D. Pei, M. Yung, D. Lin, and C. Wu, Eds., vol. 4990. Berlin, Germany: Springer, September 2007, pp. 246–255. [[online](#)]
- [42] N. Kolokotronis, K. Limniotis, and N. Kalouptsidis, "Best affine approximations of boolean functions and applications to low order approximations," in *2007 IEEE International Symposium on Information Theory – ISIT*, June 2007, pp. 1836–1840. [[online](#)]
- [43] N. Kolokotronis, K. Limniotis, and N. Kalouptsidis, "Lower bounds on sequence complexity via generalised Vandermonde determinants," in *2006 Sequences and Their Applications – SETA*, Lecture Notes in Computer Science, G. Gong, T. Hellesteth, H.-Y. Song, and K. Yang, Eds., vol. 4086. Berlin, Germany: Springer, September 2006, pp. 271–284. [[online](#)]
- [44] K. Limniotis, N. Kolokotronis, and N. Kalouptsidis, "Nonlinear complexity of binary sequences and connections with Lempel–Ziv compression," in *2006 Sequences and*

*Their Applications – SETA*, Lecture Notes in Computer Science, G. Gong, T. Hellesteth, H.-Y. Song, and K. Yang, Eds., vol. 4086. Berlin, Germany: Springer, September 2006, pp. 168–179. [[online](#)]

- [45] K. Limniotis, N. Kolokotronis, and N. Kalouptsidis, “New results on the linear complexity of binary sequences,” in *2006 IEEE International Symposium on Information Theory – ISIT*, July 2006, pp. 2003–2007. [[online](#)]
- [46] N. Kolokotronis, “Cryptographic properties of stream ciphers based on  $t$ -functions,” in *2006 IEEE International Symposium on Information Theory – ISIT*, July 2006, pp. 1604–1608. [[online](#)]
- [47] P. Rizomiliotis, N. Kolokotronis, and N. Kalouptsidis, “On the quadratic span of binary sequences,” in *2003 IEEE International Symposium on Information Theory – ISIT*, July 2003, p. 377. [[online](#)]
- [48] N. Kolokotronis, G. Gatt, and N. Kalouptsidis, “On the generation of sequences simulating higher order white noise for system identification,” in *11th European Signal Processing Conference – EUSIPCO*, vol. 1. EURASIP, September 2002, pp. 217–220. [[online](#)]
- [49] P. Rizomiliotis, N. Kolokotronis, and N. Kalouptsidis, “Construction of sequences with four-valued autocorrelation from GMW sequences,” in *2002 IEEE International Symposium on Information Theory – ISIT*, July 2002, p. 183. [[online](#)]
- [50] C. Margaritis, N. Kolokotronis, P. Papadopoulou, P. Kanellis, and D. Martakos, “A model and implementation guidelines for information security strategies in web environments,” in *Advances in Information Security Management and Small Systems Security*, IFIP Advances in Information and Communication Technology, J. H. P. Eloff, L. Labuschagne, R. von Solms, and G. Dhillon, Eds., vol. 72. Kluwer Academic Publishers, September 2001, pp. 13–34. [[online](#)]
- [51] N. Kolokotronis, P. Rizomiliotis, and N. Kalouptsidis, “First-order optimal approximation of binary sequences,” in *2001 Sequences and Their Applications – SETA*, Discrete Mathematics and Theoretical Computer Science, T. Hellesteth, P. V. Kumar, and K. Yang, Eds. Berlin, Germany: Springer, May 2001, pp. 242–256. [[online](#)]
- [52] P. Papadopoulou, N. Kolokotronis, P. Kanellis, and D. Martakos, “Conceptualizing and implementing an information security strategy for internet billing systems,” in *Advances in Infrastructure for e-Business, e-Science, and e-Education on the Internet*. Scuola Superiore Guglielmo Reiss Romoli (SSGRR), July 2000, pp. 1–9. [[online](#)]

### Technical reports

- [53] K. Limniotis, N. Kolokotronis, and N. Kalouptsidis, “Modifying boolean functions to ensure maximum algebraic immunity,” IACR Cryptology ePrint Archive, Report 2012/046, January 2012. [[online](#)]
- [54] N. Kolokotronis and K. Limniotis, “Maiorana–McFarland functions with high second-order nonlinearity,” IACR Cryptology ePrint Archive, Report 2011/212, May 2011. [[online](#)]
- [55] N. Kolokotronis, K. Limniotis, and N. Kalouptsidis, “Best quadratic approximations of cubic boolean functions,” IACR Cryptology ePrint Archive, Report 2007/037, February 2007. [[online](#)]

- [56] E. Kopanaki, N. Kolokotronis, and D. Martakos, "What is the Hellenic billing mall and how it works," *Bancassurance and Banking*, no. 3, pp. 28–36, July 2000, invited Article.

#### Forthcoming

- [57] K. Limniotis, N. Kolokotronis, and D. Kotanidis, "De Bruijn sequences and suffix arrays: analysis and constructions," under review.
- [58] K. Ntemos, J. Plata-Chaves, N. Kolokotronis, N. Kalouptsidis, and M. Moonen, "Secure information sharing in adversarial adaptive diffusion networks," under review.
- [59] N. Kolokotronis and P. Smyrli, "Multilevel constructions of ISD algorithms for solving the CSD problem," to be submitted.
- [60] N. Kolokotronis, K. Fytrakis, and N. Kalouptsidis, "Practical cooperative physical layer security strategies in wireless relay networks," under preparation.
- [61] N. Kolokotronis and K. Limniotis, "Low-order approximation attacks on block ciphers: applications in AES-128 and 3DES," under preparation.
- [62] N. Kolokotronis, "Cryptography: algorithm design and advanced cryptanalysis," (book), under preparation.

---

#### Citations to scientific work

[Google Scholar](#) reports a total number of 303 cross-citations, with h-index and i10-index being equal to 11 and 12 respectively.