

Nicholas Kolokotronis

Curriculum vitae

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

January 2024

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

- 2023–today **Professor**
University of Peloponnese, Department of Informatics and Telecommunications
- 2019–2023 **Associate professor**
University of Peloponnese, Department of Informatics and Telecommunications
- 2012–2019 **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

- 2021–today **Scientific advisory board member**
LOGOS Research and Innovation

- 2005–today **Adjunct faculty**
University of Athens, Department of Informatics and Telecommunications
- 2015–2017 **Visiting instructor**
Open University of Cyprus, Faculty of Pure and Applied Sciences
- 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
- **Privacy technologies:** privacy-preserving methods, anonymity protocols/systems, homomorphic encryption, statistical database 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

- | | | |
|------------|--|--------------------------|
| 2018–today | Big Data security, privacy and trust (co-instructor) | <i>Univ. Peloponnese</i> |
| 2018–today | Topics in cryptography and security | <i>Univ. Peloponnese</i> |
| 2005–today | Systems security (co-instructor) | <i>Univ. Athens</i> |
| 2015–2017 | 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 | Networked systems security | <i>Univ. Piraeus</i> |
| 1998–2000 | Information theory and coding (co-instructor) | <i>Univ. Athens</i> |

Undergraduate

| | | |
|------------|--|--------------------------|
| 2017–today | Discrete mathematics | <i>Univ. Peloponnese</i> |
| 2004–today | Cryptography | <i>Univ. Peloponnese</i> |
| 2004–today | Systems security | <i>Univ. Peloponnese</i> |
| 2013–2016 | Probability and statistics (co–instructor) | <i>Univ. Peloponnese</i> |
| 2015 | Mathematics II (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> |
| 2004–2005 | 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

Supervisor

| | | |
|------|---|----------------|
| 2018 | S. Brotsis, Security of consensus protocols and distributed ledger technologies | <i>ongoing</i> |
| 2018 | G. Germanos, Cyber–security and privacy in the Internet of things | <i>ongoing</i> |
| 2015 | P. Smyrli, Post–quantum cryptography: code–based cryptosystems | <i>ongoing</i> |

Advisory committee member

| | | |
|------|---|----------------|
| 2017 | E.-M. Athanasakos, Physical layer security | <i>ongoing</i> |
| 2016 | K. Katsanos, Sigmoidal programming and applications in signal processing and communications | <i>ongoing</i> |

Co–supervisor

| | | |
|------|--|------------------|
| 2013 | K. Ntemos, Stochastic games, cognitive radio networks, and security | <i>ongoing</i> |
| 2007 | K. Limniotis, Cryptographically–related complexity measures for binary sequences | <i>completed</i> |

Postgraduate

| | | |
|------|---|------------------|
| 2018 | V. Haskos, Cyber–range systems: overview and open challenges | <i>ongoing</i> |
| 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

| | | |
|------|---|------------------|
| 2018 | K.-P. Grammatikakis, Malware detection and analysis | <i>ongoing</i> |
| 2018 | C. Doukas and K. Melanitis, Topics in cryptography and security on the web | <i>ongoing</i> |
| 2016 | D. Mentesidis, Wireless communication technologies for public safety | <i>completed</i> |
| 2015 | G. Panagopoulos, Trust management models in P2P networks | <i>completed</i> |
| 2015 | G. Geramanis, Attacks on anonymity services and protocols | <i>completed</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 stream ciphers | <i>completed</i> |
| 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

| | | |
|------------|---|--------------------------|
| 2018–today | Head of the <i>cryptography and security</i> group | <i>Dept. IT</i> |
| 2018–today | Member of the Steering Committee of the postgraduate studies program in <i>Data Science</i> | <i>Dept. IT</i> |
| 2018–today | Member of the Steering Committee of the postgraduate studies program in <i>Computer Science</i> | <i>Dept. IT</i> |
| 2008–today | Member of the department's Assembly | <i>Dept. IT</i> |
| 2018 | Member of the steering committee preparing the proposal for the certification of the department's undergraduate studies program | <i>Dept. IT</i> |
| 2008–2017 | Member of the <i>algorithms, cryptography and computational logic</i> group | <i>Dept. IT</i> |
| 2011–2017 | Member of evaluation committees for the procurement of goods | <i>Univ. Peloponnese</i> |
| 2015–2016 | Member of the undergraduate studies program committee | <i>Dept. IT</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 | <i>Dept. IT</i> |

dit.uop.gr

- 2013–2015 Member of the NSRF project “information system development for the quality assurance unit at the University of Peloponnese” *Univ. Peloponnese*
- 2012–2013 Member of the undergraduate studies program committee *Dept. IT*

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

- 2017 Member of working group for the professional training of security officers in special topics of the General Data Protection Regulation (GDPR) EU 2016/679
- 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 ○ **AE**: EURASIP J. Wireless Commun. Netw. *2009–2017*

- Reviewer ○ Adv. Math. Commun. ○ IEEE Trans. Inf. Theory
- Appl. Algebra Engrg. Comm. Comput. ○ IEEE Trans. Multimedia
- Benchmarking Int. J. ○ IEEE Trans. Vehicular Tech.
- Comput. Standards Interfaces ○ Inform. Comput. Security
- Cryptogr. Commun. ○ Inform. Process. Lett.
- Des. Codes Cryptogr. ○ Int. J. Commun. Syst.
- Discrete Appl. Math. ○ Int. J. Comput. Math.
- Discrete Math. ○ Int. J. Electron. Governance
- EURASIP J. Wireless Commun. Netw. ○ J. Appl. Math. Comput.
- Finite Fields Appl. ○ J. Complexity
- IEEE Commun. Lett. ○ J. Comput. Sci. Tech.
- IEEE Consum. Electron. Mag. ○ J. Signal Image Video Process.
- IEEE Trans. Commun. ○ Security Commun. Netw.
- IEEE Trans. Ind. Informat. ○ Signal Process.
- IEEE Trans. Inf. Forensics & Security

- TPC member ○ E–DEM (Conf. e–Democracy Security Priv. Trust) *2013, 2015, 2017*
- DSP (Int. Conf. Digit. Signal Process.) *2009, 2011*
- EUSIPCO (Eur. Signal Process. Conf.) *1998, 2008*
- ICASSP (Int. Conf. Acoust. Speech Signal Process.) *2012*
- ICCS (Int. Conf. Comput. Sci.) *2006–2007*

| | |
|--|------------------------|
| ○ IEEE GLOBECOM (Commun. Inf. Security Symp.) | 2009 |
| ○ IEEE ICC (Int. Conf. Commun.) | 2011 |
| ○ IEEE ISCAS (Int. Symp. Circuits Syst.) | 2003 |
| ○ IEEE ISIT (Int. Symp. Inf. Theory) | 2003, 2011, 2013, 2015 |
| ○ IEEE MELECON (Mediterranean Electrotech. Conf.) | 2016 |
| ○ IEEE WDFIA (Wkshp Digit. Forensics Incident Anal.) | 2007–2010 |
| ○ ISC (Int. Conf. Inf. Security) | 2017 |
| ○ ISPEC (Inform. Security Pract. Experience Conf.) | 2014 |
| ○ MCIS (Mediterranean Conf. Inf. Syst.) | 2009 |
| ○ PARA (Wkshp SoA Sci. Parallel Comput.) | 2006 |
| ○ PCI (Panhellenic Conf. Inform.) | 2010 |
| ○ STM (Int. Wkshp Security Trust Manag.) | 2018 |
| Publicity ○ STM (Int. Wkshp Security Trust Manag.) | 2018 |

Projects, grants

Grants

- 2006–2008 Study of complexity and pseudorandomness properties in symmetric encryption algorithms
Coordinator: University of Athens *Grant no.:* 70/3/8470
Funding: British Council *Budget:* 16,0 K€
Responsibilities: Principal investigator
- 2005 Study of stream ciphers in symmetric cryptography
Coordinator: University of Athens *Grant no.:* 70/4/7818
Funding: University of Athens *Budget:* 4,5 K€
Responsibilities: Principal investigator

Research projects

- 2021–2024 ELECTRON: Resilient and self-healed electrical power nanogrid
Coordinator: Instrasoft International *Grant no.:* 101021936 (SU-DS04-2018-2020)
Funding: European Commission, H2020 *Budget:* 10,2 M€
Responsibilities: Team member
- 2020–2023 TERMINET: Next generation smart interconnected IoT
Coordinator: University of Western Macedonia *Grant no.:* 957406 (ICT-56-2020)
Funding: European Commission, H2020 *Budget:* 8,0 M€
Responsibilities: Team member
- 2019–2022 FORESIGHT: Advanced cyber–security simulation platform for preparedness training in aviation, power–grid and naval environments
Coordinator: European Dynamics SA *Grant no.:* 833673 (SU-DS01-2018)
Funding: European Commission, H2020 *Budget:* 6,0 M€
Responsibilities: Team leader, work package leader, project technical manager – also among the key members leading the proposal's preparation/ drafting

- 2018–2021 CYBER-TRUST: advanced cyber–threat intelligence, detection, and mitigation platform for a trusted Internet of things
Coordinator: Center for Security Studies *Grant no.:* 786698 (DS-07-2017)
Funding: European Commission, H2020 *Budget:* 3,0 M€
Responsibilities: Team leader, work package leader, project technical manager – also responsible for the preparation/ drafting of the proposal and its key innovative ideas (**ranked 1st among 63 proposals with score 15/15**)
- 2013–2016 HANDICAMS: heterogeneous ad–hoc networks for distributed, cooperative, and adaptive multimedia signal processing
Coordinator: Katholieke Univ. Leuven *Grant no.:* FET–323944
Funding: European Commission, FP7 *Budget:* 2,0 M€
Responsibilities: Team member, work package leader
- 2012–2015 ART–IN–SPACE: adaptive, robust to threats, immune to nonlinearities, sparse opportunistic cognitive radio
Coordinator: University of Athens *Grant no.:* 70/3/11918
Funding: NSRF Excellence Program *Budget:* 157,5 K€
Responsibilities: Team member, work package leader
- 2012–2015 SWINCOM: secure wireless nonlinear communications at the physical layer
Coordinator: University of Athens *Grant no.:* 70/3/11668
Funding: NSRF Thalys Program *Budget:* 512,8 K€
Responsibilities: Team leader, work package leader – also responsible for the preparation and drafting of the proposal
- 2004–2007 ECON–TISP: application of economic theories to design and develop telecommunications and information systems and products
Coordinator: University of Athens *Grant no.:* 56/90/7425
Funding: Community Support Frwk III *Budget:* 90,0 K€
Responsibilities: Principal investigator
- 2004–2007 SECURE– JUSTICE: secure communication and collaboration framework for the judicial cooperation environment
Coordinator: Project Automation SpA *Grant no.:* IST-2002-507188
Funding: European Commission, FP6 *Budget:* 5,4 M€
Responsibilities: Team manager
- 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 no.:* IST-2000-31083
Funding: European Commission, FP5 *Budget:* 2,0 M€
Responsibilities: Project manager
- 2002–2005 ICTE–PAN: methodologies and tools for building intelligent collaboration and transaction environments in public administration networks
Coordinator: European Dynamics SA *Grant no.:* IST-2001-35120
Funding: European Commission, FP5 *Budget:* 3,2 M€
Responsibilities: Team member
- 2000–2001 CHANNEL SOUNDER: development of an intelligent measurement device for the multidimensional characterization of broadband radio channels
Coordinator: Nat. Tech. Univ. Athens *Grant no.:* 61/1189
Funding: General Secretariat R&T *Budget:* 176,1 K€
Responsibilities: Team member

- 1999–2001 BILLING MALL: development of an integrated e-commerce platform for secure billing management in subscription services
Coordinator: University of Athens *Grant no.:* 70/3/4483
Funding: General Secretariat R&T *Budget:* 1,1 M€
Responsibilities: Team member
- 1996–1998 EUROMED: technologies for founding of a european telemedical information society
Coordinator: Nat. Tech. Univ. Athens *Grant no.:* 70/3/2723
Funding: European Commission, TEDIS *Budget:* 1,6 M€
Responsibilities: Team member

Consulting projects

- 2007 Technical action plan and specifications of supplementary technical infrastructures for operating the General Business Register (GBR)
Coordinator: University of Athens *Grant no.:* 70/3/9291
Funding: General Secretariat Comm. *Budget:* –
Responsibilities: Team member
- 2000 Consulting services for supporting the Public Power Corporation (PPC) enter the telecommunications market
Coordinator: University of Athens *Grant no.:* 70/3/5328
Funding: Public Power Corporation *Budget:* –
Responsibilities: Team member
- 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 no.:* 70/3/5255
Funding: Nat. Comm. Telecomm. Posts *Budget:* –
Responsibilities: Team member
- 1999 Development of telecommunications security policies
Coordinator: University of Athens *Grant no.:* 70/3/4706
Funding: Ministry Transp. Telecomm. *Budget:* –
Responsibilities: Team member

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, monographs, book editions

- [1] S. Shiaeles and N. Kolokotronis, *Proceedings of the 2022 IEEE International Conference on Cyber Security and Resilience (CSR)*. IEEE Press, July 2022. [[online](#)]
- [2] G. Sargsyan, D. Kavallieros, and N. Kolokotronis, *Security Technologies and Methods for Advanced Cyber Threat Intelligence, Detection and Mitigation*. Now Publishers, March 2022. [[online](#)]
- [3] S. Shiaeles, N. Kolokotronis, and E. Bellini, *Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience (CSR)*. IEEE Press, July 2021. [[online](#)]
- [4] S. Shiaeles and N. Kolokotronis, *Internet of Things, Threats, Landscape, and Countermeasures*. CRC Press, April 2021. [[online](#)]
- [5] N. Kolokotronis and S. Shiaeles, *Cyber-Security Threats, Actors, and Dynamic Mitigation*. CRC Press, April 2021. [[online](#)]
- [6] P. Kanellis, E. Kiountouzis, N. Kolokotronis, and D. Martakos, *Digital crime and forensic science in cyberspace*. IGI Global Publishing, April 2006. [[online](#)]
- [7] 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](#)]

Book chapters and edited volumes

- [8] A. Varelias, K. Limniotis, and N. Kolokotronis, “Cryptographic properties of boolean functions generating similar De Bruijn sequences,” in *Analysis, Cryptography and Information Science*, N. J. Daras, P. M. Pardalos, and M. T. Rassias, Eds. World Scientific Publishing, 2023, pp. 233–262, **Accepted**. [[online](#)]
- [9] E. Chaskos, J. Diakoumakos, N. Kolokotronis, and G. Lepouras, “Gamification mechanisms in cyber range and cyber security training environments,” in *Handbook of Research on Gamification Dynamics and User Experience Design*, O. Bernardes, V. Amorim, and A. Carrizo Moreira, Eds. IGI Global Publishing, May 2022, pp. 363–383. [[online](#)]
- [10] C.-M. Mathas, C. Vassilakis, N. Kolokotronis, and K. P. Grammatikakis, “Trust management system architecture for the Internet of things,” in *Security Technologies and Methods for Advanced Cyber Threat Intelligence, Detection and Mitigation*, G. Sargsyan, D. Kavallieros, and N. Kolokotronis, Eds. Now Publishers, March 2022, pp. 130–160. [[online](#)]
- [11] S. Brotsis, N. Kolokotronis, and K. Limniotis, “Towards post-quantum blockchain platforms,” in *Security Technologies and Methods for Advanced Cyber Threat Intelligence*,

- Detection and Mitigation*, G. Sargsyan, D. Kavallieros, and N. Kolokotronis, Eds. Now Publishers, March 2022, pp. 105–130. [[online](#)]
- [12] K. P. Grammatikakis, I. Koufos, and N. Kolokotronis, "Moving-target defense techniques for mitigating sophisticated IoT threats," in *Security Technologies and Methods for Advanced Cyber Threat Intelligence, Detection and Mitigation*, G. Sargsyan, D. Kavallieros, and N. Kolokotronis, Eds. Now Publishers, March 2022, pp. 51–73. [[online](#)]
- [13] K. P. Grammatikakis and N. Kolokotronis, "Attack graph generation," in *Cyber-Security Threats, Actors, and Dynamic Mitigation*, N. Kolokotronis and S. Shiaeles, Eds. CRC Press, April 2021, pp. 281–334. [[online](#)]
- [14] I. Koufos, N. Kolokotronis, and K. Limniotis, "Dynamic risk management," in *Cyber-Security Threats, Actors, and Dynamic Mitigation*, N. Kolokotronis and S. Shiaeles, Eds. CRC Press, April 2021, pp. 247–280. [[online](#)]
- [15] K. Limniotis and N. Kolokotronis, "Cryptography threats," in *Cyber-Security Threats, Actors, and Dynamic Mitigation*, N. Kolokotronis and S. Shiaeles, Eds. CRC Press, April 2021, pp. 123–158. [[online](#)]
- [16] K. P. Grammatikakis and N. Kolokotronis, "System threats," in *Cyber-Security Threats, Actors, and Dynamic Mitigation*, N. Kolokotronis and S. Shiaeles, Eds. CRC Press, April 2021, pp. 81–122. [[online](#)]
- [17] D. Kavallieros, G. Germanos, and N. Kolokotronis, "Profiles of cyber-attackers and attacks," in *Cyber-Security Threats, Actors, and Dynamic Mitigation*, N. Kolokotronis and S. Shiaeles, Eds. CRC Press, April 2021, pp. 1–26. [[online](#)]
- [18] A. Grigoriadis, E. Darra, D. Kavallieros, E. Chaskos, N. Kolokotronis, and X. Bellekens, "Cyber ranges: The new training era in the cybersecurity and digital forensics world," in *Technology Development for Security Practitioners, Security Informatics and Law Enforcement*, B. Akhgar, D. Kavallieros, and E. Sdongos, Eds. Springer, 2021, pp. 97–117. [[online](#)]
- [19] V. G. Bilali, D. Kavallieros, G. Kokkinis, P. Kolovos, D. Katsoulis, T. Anatolitis, N. Georgiou, N. Kolokotronis, O. Gkotsopoulou, C. Pavue, S. Cuomo, S. Naldini, S. Shiaeles, and G. Sargsyan, "Cyber-Trust: Meeting the needs of information sharing between ISPs and LEAs," in *Technology Development for Security Practitioners, Security Informatics and Law Enforcement*, B. Akhgar, D. Kavallieros, and E. Sdongos, Eds. Springer, 2021, pp. 73–95. [[online](#)]
- [20] N. Kolokotronis, K. Limniotis, and P. Rizomiliotis, "Applied cryptography," in *Information and Systems Security in Cyber-Space*, S. K. Katsikas, S. Gritzalis, and C. Lambrinoudakis, Eds. NewTech Publications, 2021, pp. 235–282. [[online](#)]
- [21] N. Kolokotronis, S. Shiaeles, E. Bellini, L. Charalambous, D. Kavallieros, O. Gkotsopoulou, C. Pavue, A. Bellini, and G. Sargsyan, "Cyber-Trust: The shield for IoT cyber-attacks," in *Resilience and Hybrid Threats*, NATO Science for Peace and Security Series – D: Information and Communication Security, I. Linkov, L. Roslycky, and B. D. Trump, Eds. IOS Press, 2019, vol. 55, pp. 76–93, Research Article. [[online](#)]
- [22] K. Limniotis, N. Kolokotronis, and D. Kotanidis, "De Bruijn sequences and suffix arrays: analysis and constructions," in *Modern Discrete Mathematics and Analysis: With Applications in Cryptography, Information Systems, and Modelling*, N. J. Daras and T. M. Rassias, Eds. Springer, 2018, pp. 257–276. [[online](#)]

- [23] 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](#)]
- [24] 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](#)]
- [25] 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](#)]
- [26] 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. Lambrinoudakis, L. Mitrou, S. Gritzalis, and S. K. Katsikas, Eds. Papatotiriou Pubs, 2010, pp. 123–145. [[online](#)]
- [27] 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

- [28] S. Brotsis, K. P. Grammatikakis, D. Kavallieros, A. I. Mazilu, N. Kolokotronis, K. Limniotis, and C. Vassilakis, "Blockchain meets internet of things (IoT) forensics: A unified framework for iot ecosystems," *Internet of Things*, vol. 24, pp. 1–25, October 2023. [[online](#)]
- [29] P. Sotiropoulos, C.-M. Mathas, C. Vassilakis, and N. Kolokotronis, "A software vulnerability management framework for the minimization of system attack surface and risk," *Electronics*, vol. 12, no. 10, pp. 1–21, May 2023. [[online](#)]
- [30] G. Achilleos, K. Limniotis, and N. Kolokotronis, "Exploring the personal data processing in video conferencing apps," *Electronics*, vol. 12, no. 5, pp. 1–25, March 2023. [[online](#)]
- [31] G. Bendiab, A. Hameurlaine, G. Germanos, N. Kolokotronis, and S. Shiaeles, "Autonomous vehicles security: Challenges and solutions using blockchain and artificial intelligence," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–24, January 2023. [[online](#)]
- [32] I. Tzinis, K. Limniotis, and N. Kolokotronis, "Evaluating the performance of post-quantum secure algorithms in the TLS protocol," *Journal of Surveillance, Security and Safety*, vol. 3, pp. 101–127, September 2022. [[online](#)]
- [33] J. R. Rose, M. Swann, K. P. Grammatikakis, I. Koufos, G. Bendiab, S. Shiaeles, and N. Kolokotronis, "IDERES: Intrusion detection and response system using machine learning and attack graphs," *Journal of Systems Architecture*, vol. 131, pp. 1–12, October 2022. [[online](#)]
- [34] S. Monogios, K. Magos, K. Limniotis, N. Kolokotronis, and S. Shiaeles, "Privacy issues in Android applications: The cases of GPS navigators and fitness trackers," *International Journal of Electronic Governance*, vol. 14, no. 1/2, pp. 83–111, May 2022. [[online](#)]
- [35] C.-M. Mathas, C. Vassilakis, N. Kolokotronis, C. C. Zarakovitis, and M.-A. Kourtis, "On the design of IoT security: Analysis of software vulnerabilities for smart grids," *Energies*, vol. 14, no. 10, pp. 1–27, May 2021. [[online](#)]

- [36] S. Brotsis, K. Limniotis, G. Bendiab, N. Kolokotronis, and S. Shiaeles, "On the suitability of blockchain platforms for IoT applications: Architectures, security, privacy, and performance," *Computer Networks*, vol. 191, pp. 1–29, May 2021, 108005. [[online](#)]
- [37] N. Dalezios, S. Shiaeles, N. Kolokotronis, and B. Ghita, "Digital forensics cloud log unification: Implementing CADF in Apache CloudStack," *Journal of Information Security and Applications*, vol. 54, pp. 1–9, October 2020. [[online](#)]
- [38] K. Fytrakis, N. Kolokotronis, K. Katsanos, and N. Kalouptsidis, "Optimal cooperative strategies for PHY security maximization subject to SNR constraints," *IEEE Access*, vol. 8, pp. 119312–119323, July 2020. [[online](#)]
- [39] A. Ramsdale, S. Shiaeles, and N. Kolokotronis, "A comparative analysis of cyber-threat intelligence sources, formats and languages," *Electronics*, vol. 9, no. 5, pp. 1–22, May 2020. [[online](#)]
- [40] K. Limniotis and N. Kolokotronis, "The error linear complexity spectrum as a cryptographic criterion of Boolean functions," *IEEE Transactions on Information Theory*, vol. 65, no. 12, pp. 8345–8356, December 2019. [[online](#)]
- [41] N. Kolokotronis, K. Limniotis, S. Shiaeles, and R. Griffiths, "Secured by blockchain: Safeguarding Internet of things devices," *IEEE Consumer Electronics Magazine*, vol. 8, no. 3, pp. 28–34, May 2019, Special issue: *blockchain technologies for consumer electronics*. [[online](#)]
- [42] K. Limniotis and N. Kolokotronis, "Boolean functions with maximum algebraic immunity: further extensions of the Carlet–Feng construction," *Designs, Codes and Cryptography*, vol. 86, no. 8, pp. 1685–1706, August 2018. [[online](#)]
- [43] K. Ntemos, J. Plata-Chaves, N. Kolokotronis, N. Kalouptsidis, and M. Moonen, "Secure information sharing in adversarial adaptive diffusion networks," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 4, no. 1, pp. 111–124, March 2018, Special issue: *distributed signal processing for security and privacy in networked cyber-physical systems*. [[online](#)]
- [44] 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](#)]
- [45] 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](#)]
- [46] 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](#)]
- [47] 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](#)]
- [48] 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](#)]

- [49] 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](#)]
- [50] N. Kolokotronis, "Cryptographic properties of nonlinear pseudorandom number generators," *Designs, Codes and Cryptography*, vol. 46, no. 3, pp. 353–363, March 2008. [[online](#)]
- [51] 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](#)]
- [52] 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](#)]
- [53] 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](#)]
- [54] 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](#)]
- [55] 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](#)]
- [56] 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](#)]
- [57] 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](#)]
- [58] 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)

- [59] A. Papathanasiou, G. Germanos, N. Kolokotronis, and E. Glavas, "Cognitive email analysis with automated decision support for business email compromise prevention," in *8th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference – SEEDA-CECNSM*. IEEE, November 2023, pp. 1–5. [[online](#)]
- [60] P. Sotiropoulos, C.-M. Mathas, C. Vassilakis, and N. Kolokotronis, "Minimizing software-rooted risk through library implementation selection," in *IEEE International Conference on Cyber Security and Resilience – CSR*. IEEE, July 2023, pp. 496–502. [[online](#)]
- [61] N. Kolokotronis, M. Dareioti, S. Shiaeles, and E. Bellini, "An intelligent platform for threat assessment and cyber-attack mitigation in IoMT ecosystems," in *2022 IEEE Global*

Communications Conference – GLOBECOM, Workshop on Edge-AI and IoT for Connected Health. IEEE, December 2022, pp. 541–546. [[online](#)]

- [62] K. P. Grammatikakis, I. Koufos, and N. Kolokotronis, “A collaborative intelligent intrusion response framework for smart electrical power and energy systems,” in *17th International Conference on Availability, Reliability and Security – ARES*. ACM, August 2022, pp. 1–10. [[online](#)]
- [63] E. Chaskos, J. Diakoumakos, N. Kolokotronis, and G. Lepouras, “Handling critical infrastructures in federation of cyber ranges: A classification model,” in *17th International Conference on Availability, Reliability and Security – ARES*. ACM, August 2022, pp. 1–9. [[online](#)]
- [64] S. Brotsis and N. Kolokotronis, “Blockchain-enabled digital forensics for the IoT: Challenges, features, and current frameworks,” in *IEEE International Conference on Cyber Security and Resilience – CSR*. IEEE, July 2022, pp. 131–137. [[online](#)]
- [65] N. Koutsouris, C. Vassilakis, and N. Kolokotronis, “Cyber-security training evaluation metrics,” in *IEEE International Conference on Cyber Security and Resilience – CSR*. IEEE, July 2021, pp. 192–197. [[online](#)]
- [66] J. Diakoumakos, E. Chaskos, N. Kolokotronis, and G. Lepouras, “Cyber-range federation and cyber-security games: A gamification scoring model,” in *IEEE International Conference on Cyber Security and Resilience – CSR*. IEEE, July 2021, pp. 186–191. [[online](#)]
- [67] E. Pantelidis, G. Bendiab, S. Shiaeles, and N. Kolokotronis, “Insider threat detection using deep autoencoder and variational autoencoder neural networks,” in *IEEE International Conference on Cyber Security and Resilience – CSR*. IEEE, July 2021, pp. 129–134. [[online](#)]
- [68] K. Grammatikakis, I. Koufos, N. Kolokotronis, C. Vassilakis, and S. Shiaeles, “Understanding and mitigating banking trojans: From Zeus to Emotet,” in *IEEE International Conference on Cyber Security and Resilience – CSR*. IEEE, July 2021, pp. 121–128. [[online](#)]
- [69] J. R. Rose, M. Swann, G. Bendiab, S. Shiaeles, and N. Kolokotronis, “Intrusion detection using network traffic profiling and machine learning for IoT,” in *7th IEEE International Conference on Network Softwarization – NetSoft, SecSoft workshop*, K. Shiimoto, Y. Kim, C. E. Rothenberg, B. Martini, E. Oki, B. Choi, N. Kamiyama, and S. Secci, Eds. IEEE, June 2021, pp. 409–415. [[online](#)]
- [70] D. Buckley, G. Bendiab, S. Shiaeles, N. Savage, and N. Kolokotronis, “CHAINGE: A blockchain solution to automate payment detail updates to subscription services,” in *IEEE International Conference on Communications Workshops – ICC*. IEEE, June 2021, pp. 1–6. [[online](#)]
- [71] G. Kermezis, K. Limniotis, and N. Kolokotronis, “User-generated pseudonyms through Merkle trees,” in *9th Annual Privacy Forum – APF, Lecture Notes in Computer Science*, N. Gruschka, L. F. C. Antunes, K. Rannenber, and P. Drogkaris, Eds., vol. 12703. Springer, June 2021, pp. 89–105. [[online](#)]
- [72] G. Germanos, D. Kavallieros, N. Kolokotronis, and N. Georgiou, “Privacy issues in voice assistant ecosystems,” in *2020 IEEE World Congress on Services – SERVICES*. IEEE, October 2020, pp. 205–212. [[online](#)]

- [73] S. Brotsis, N. Kolokotronis, K. Limniotis, G. Bendiab, and S. Shiaeles, "On the security and privacy of Hyperledger Fabric: Challenges and open issues," in *2020 IEEE World Congress on Services – SERVICES*. IEEE, October 2020, pp. 197–204. [[online](#)]
- [74] C. Mathas, C. Vassilakis, and N. Kolokotronis, "A trust management system for the IoT domain," in *2020 IEEE World Congress on Services – SERVICES*. IEEE, October 2020, pp. 183–188. [[online](#)]
- [75] G. Bendiab, K. Grammatikakis, I. Koufos, N. Kolokotronis, and S. Shiaeles, "Advanced metering infrastructures: Security risks and mitigation," in *15th International Conference on Availability, Reliability and Security – ARES*, M. Volkamer and C. Wressnegger, Eds. ACM, August 2020, pp. 1–8. [[online](#)]
- [76] C. Mathas, K. Grammatikakis, C. Vassilakis, N. Kolokotronis, V. Bilali, and D. Kavallieros, "Threat landscape for smart grid systems," in *15th International Conference on Availability, Reliability and Security – ARES*, M. Volkamer and C. Wressnegger, Eds. ACM, August 2020, pp. 1–7. [[online](#)]
- [77] S. Brotsis, N. Kolokotronis, K. Limniotis, and S. Shiaeles, "On the security of permissioned blockchain solutions for IoT applications," in *6th IEEE Conference on Network Softwarization – NetSoft, SecSoft Workshop*, F. D. Turck, P. Chemouil, T. Wauters, M. F. Zhani, W. Cerroni, R. Pasquini, and Z. Zhu, Eds. IEEE, June 2020, pp. 465–472. [[online](#)]
- [78] G. Bendiab, S. Shiaeles, A. Alruban, and N. Kolokotronis, "IoT malware network traffic classification using visual representation and deep learning," in *6th IEEE Conference on Network Softwarization – NetSoft, SecSoft Workshop*, F. D. Turck, P. Chemouil, T. Wauters, M. F. Zhani, W. Cerroni, R. Pasquini, and Z. Zhu, Eds. IEEE, June 2020, pp. 444–449. [[online](#)]
- [79] F. Alsakran, G. Bendiab, S. Shiaeles, and N. Kolokotronis, "Intrusion detection systems for smart home IoT devices: Experimental comparison study," in *7th International Symposium on Security in Computing and Communications – SSCC*, Communications in Computer and Information Science, S. M. Thampi, G. M. Pérez, R. K. L. Ko, and D. B. Rawat, Eds., vol. 1208. Springer, December 2019, pp. 87–98. [[online](#)]
- [80] S. Monogios, K. Limniotis, N. Kolokotronis, and S. Shiaeles, "A case study of intra-library privacy issues on android GPS navigation apps," in *8th International Conference on E-Democracy – e-Democracy*, Communications in Computer and Information Science, S. K. Katsikas and V. Zorkadis, Eds., vol. 1111. Springer, December 2019, pp. 34–48. [[online](#)]
- [81] R. Shire, S. Shiaeles, K. Bendiab, B. V. Ghita, and N. Kolokotronis, "Malware squid: A novel IoT malware traffic analysis framework using convolutional neural network and binary visualisation," in *19th International Conference on Internet of Things, Smart Spaces, and Next Generation Networks and Systems – NEW2AN*, Lecture Notes in Computer Science, O. Galinina, S. Andreev, S. I. Balandin, and Y. Koucheryavy, Eds., vol. 11660. Springer, August 2019, pp. 65–76. [[online](#)]
- [82] T. Chantzios, P. Koloveas, S. Skiadopoulos, N. Kolokotronis, C. Tryfonopoulos, V. Bilali, and D. Kavallieros, "The quest for the appropriate cyber-threat intelligence sharing platform," in *8th International Conference on Data Science, Technology and Applications – DATA*, S. Hammoudi, C. Quix, and J. Bernardino, Eds. SciTePress, July 2019, pp. 369–376. [[online](#)]

- [83] S. Shiaeles, N. Kolokotronis, and E. Bellini, "IoT vulnerability data crawling and analysis," in *2019 IEEE World Congress on Services – SERVICES*, C. K. Chang, P. Chen, M. Goul, K. Oyama, S. Reiff-Marganiec, Y. Sun, S. Wang, and Z. Wang, Eds. IEEE, July 2019, pp. 78–83. [[online](#)]
- [84] N. Kolokotronis, S. Brotsis, G. Germanos, C. Vassilakis, and S. Shiaeles, "On blockchain architectures for trust-based collaborative intrusion detection," in *2019 IEEE World Congress on Services – SERVICES*, C. K. Chang, P. Chen, M. Goul, K. Oyama, S. Reiff-Marganiec, Y. Sun, S. Wang, and Z. Wang, Eds. IEEE, July 2019, pp. 21–28. [[online](#)]
- [85] C. Constantinides, S. Shiaeles, B. V. Ghita, and N. Kolokotronis, "A novel online incremental learning intrusion prevention system," in *10th IFIP International Conference on New Technologies, Mobility and Security – NTMS*. IEEE, June 2019, pp. 1–6. [[online](#)]
- [86] S. Brotsis, N. Kolokotronis, K. Limniotis, S. Shiaeles, D. Kavallieros, E. Bellini, and C. Pavué, "Blockchain solutions for forensic evidence preservation in IoT environments," in *5th IEEE International Conference on Network Softwarization – NetSoft, SecSoft Workshop*, C. Jacquenet, F. D. Turck, P. Chemouil, F. Esposito, O. Festor, W. Cerroni, and S. Secci, Eds. IEEE, June 2019, pp. 110–114. [[online](#)]
- [87] O. Gkotsopoulou, E. Charalambous, K. Limniotis, P. Quinn, D. Kavallieros, G. Sargsyan, S. Shiaeles, and N. Kolokotronis, "Data protection by design for cybersecurity systems in a smart home environment," in *5th IEEE International Conference on Network Softwarization – NetSoft, SecSoft Workshop*, C. Jacquenet, F. D. Turck, P. Chemouil, F. Esposito, O. Festor, W. Cerroni, and S. Secci, Eds. IEEE, June 2019, pp. 101–109. [[online](#)]
- [88] I. Baptista, S. Shiaeles, and N. Kolokotronis, "A novel malware detection system based on machine learning and binary visualization," in *53rd IEEE International Conference on Communications – ICC, DDINS Workshop*. IEEE, May 2019, pp. 1–6. [[online](#)]
- [89] K. Bendiab, N. Kolokotronis, S. Shiaeles, and S. Boucherkha, "A novel blockchain-based trust model for cloud identity management," in *16th IEEE International Conference on Dependable, Autonomic and Secure Computing – DASC*. IEEE Computer Society, August 2018, pp. 724–729. [[online](#)]
- [90] K.-P. Grammatikakis, A. Ioannou, S. Shiaeles, and N. Kolokotronis, "Are cracked applications really free? An empirical analysis on Android devices," in *16th IEEE International Conference on Dependable, Autonomic and Secure Computing – DASC*. IEEE Computer Society, August 2018, pp. 730–735. [[online](#)]
- [91] 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, pp. 2591–2595. [[online](#)]
- [92] 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](#)]
- [93] N. Kolokotronis and M. Athanasakos, "Improving physical layer security in DF relay networks via two-stage cooperative jamming," in *24th European Signal Processing Conference – EUSIPCO*. EURASIP, August 2016, pp. 1173–1177. [[online](#)]

- [94] 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](#)]
- [95] 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](#)]
- [96] 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](#)]
- [97] 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](#)]
- [98] 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, TPLS Workshop*, December 2014, pp. 1483–1488. [[online](#)]
- [99] 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](#)]
- [100] 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](#)]
- [101] 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](#)]
- [102] 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](#)]
- [103] 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](#)]
- [104] 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](#)]
- [105] 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](#)]
- [106] 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](#)]

- [107] 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](#)]
- [108] 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](#)]
- [109] 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](#)]
- [110] 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](#)]
- [111] 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](#)]
- [112] 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](#)]
- [113] 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](#)]
- [114] 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](#)]
- [115] 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](#)]
- [116] 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](#)]
- [117] 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](#)]

- [118] 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. Helleseth, P. V. Kumar, and K. Yang, Eds. Berlin, Germany: Springer, May 2001, pp. 242–256. [[online](#)]
- [119] 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 – SSRR, July 2000, pp. 1–9. [[online](#)]

Technical reports

- [120] N. Kolokotronis and S. Shiaeles, "Effective response and mitigation of advanced cyber-attacks via an intelligent cyber-defence framework," Open Access Government, September 2019. [[online](#)]
- [121] S. Shiaeles and N. Kolokotronis, "Cyber-Trust: Safeguarding IoT and building trust through blockchain," Open Access Government, September 2019. [[online](#)]
- [122] 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](#)]
- [123] N. Kolokotronis and K. Limniotis, "Maiorana–McFarland functions with high second-order nonlinearity," IACR Cryptology ePrint Archive, Report 2011/212, May 2011. [[online](#)]
- [124] N. Kolokotronis, K. Limniotis, and N. Kalouptsidis, "Best quadratic approximations of cubic Boolean functions," IACR Cryptology ePrint Archive, Report 2007/037, February 2007. [[online](#)]
- [125] 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

- [126] S. Brotsis, P. Leonis, K. Ntouros, A. I. Mazilu, N. Kolokotronis, and C. Vassilakis, "A blockchain-based trust management system for collaborative intrusion detection," pp. 1–19, under preparation.
- [127] J. Diakoumakos, E. Chaskos, N. Kolokotronis, and G. Lepouras, "Cyber-security gamification in federation of cyber-ranges: Design, implementation, and evaluation," pp. 1–19, under preparation.

Citations to scientific work

The [Google Scholar](#) reports a total number of **1939** citations to the published research work, with bibliometric indexes

- h-index equal to **24**,
- i10-index equal to **45**.

A significant part of the citations have been recorded in the last 4 years.