Curriculum vitae with track record
(for established researchers)

PERSONAL INFORMATION

Gligoroski, Danilo
Date of birth: *08.06.1967*
Sex: Male
Nationality: Macedonian

Researcher unique identifier(s) (ORCID, ResearcherID, etc.): H-9238-2016
URL for personal web site: http://www.ntnu.edu/employees/danilog

EDUCATION

1997   PhD
          Faculty of Natural Sciences and Mathematics, Ss Cyril and Methodious University,
          Skopje, Macedonia
1993   Master
          Faculty of Natural Sciences and Mathematics, Ss Cyril and Methodious University,
          Skopje, Macedonia

CURRENT AND PREVIOUS POSITIONS

2008 - ...   Professor
                  Faculty of Information Technology, Mathematics and Electrical Engineering,
                  Department of Telematics, NTNU, Norwegian University of Science and
                  Technology, Trondheim, Norway
2005-2008   Postdoc
                  Q2S Center of Excellence, NTNU, Norwegian University of Science and
                  Technology, Trondheim, Norway
1997-2005   Assistant Professor
                  Faculty of Natural Sciences and Mathematics, Ss Cyril and Methodious University,
                  Skopje, Macedonia

FELLOWSHIPS AND AWARDS

2016   Best Paper Award for the paper *"A 16-bit reconfigurable encryption processor for Pi-Cipher",* 23rd Reconfigurable Architectures Workshop, IEEE Computer Society
2012   Best Paper Award for the paper *"Construction of Optimal 4-bit S-boxes by Quasigroups of Order 4",* SECURWARE 2012, International Academy, Research and Industry Association (IARIA) 2012
2007   Achievment Award at The 2007 World Congres in Computer Science, Computer Engineering, and Applied Computing, WORLDCOMP'07

MOBILITY

2014   Visit to Laboratoire d'Informatique de Paris 6 (LIP6), Universite Pierre et Marie Curie. Sabbatical leave.

2014   Visit to Centre for Research on Cryptography and Security (CRoCS), Faculty of Informatics, Masaryk University, Brno, Czech Republic. Sabbatical leave.

2004   Visit to University of California at San Diego, Institute of Nonlinear Science, Research Grant under Exchange Visitor Program, Nr: P-1-02849

2004   Visit to University of Twente, Faculty of Electrical Engineering, Mathematics and Computer Science, Department of Computer Science, TEMPUS Individual Mobility Grant IMG-FYR3013-2003.

SUPERVISION OF GRADUATE STUDENTS AND RESEARCH FELLOWS

Number of Postdocs: 1
Number of graduated PhD students: 4
Number of graduated Master Students: >50

TEACHING ACTIVITIES (if applicable)

2015   Professor, "Ethical Hacking", Faculty of Information Technology, Mathematics and Electrical Engineering, Department of Telematics, NTNU, Norwegian University of Science and Technology, Trondheim, Norway

2008 – 2013   Professor, "Information Security", Faculty of Information Technology, Mathematics and Electrical Engineering, Department of Telematics, NTNU, Norwegian University of Science and Technology, Trondheim, Norway

2002 – 2005   Assistant professor, "Security in Computer Systems and Cryptography", Faculty of Natural Sciences and Mathematics, Ss Cyril and Methodious University, Skopje, Macedonia

2002 – 2005   Assistant professor, "Data Structures", Faculty of Natural Sciences and Mathematics, Ss Cyril and Methodious University, Skopje, Macedonia

1997 – 2002   Assistant professor, "Discrete Mathematics", Faculty of Natural Sciences and Mathematics, Ss Cyril and Methodious University, Skopje, Macedonia

ORGANISATION OF SCIENTIFIC MEETINGS

2015   General Co-Chair, Information Security Conference (ISC 2015), September 9-11, 2015, Trondheim, Norway, 70 participants

INSTITUTIONAL RESPONSIBILITIES

2008 – 2016   Academic coordinator for the Erasmus Mundus Master Programme in Security and Mobile Computing – NordSecMob, NTNU, Norwegian University of Science and Technology, Trondheim, Norway

REVIEWER FOR

NordSec, NISK-Norsk Informasjonssikkerhetskonferanse, International Journal of Network Security, Journal of Systems and Software – Elsevier, Parallel Computing – Elsevier, Physics Letters A – Elsevier, Mathematical Reviews, International Workshop on Security and

Communication Networks, Communication and Information Security (IASTED CIS), Technical Program Committee for ICCCN, Network Security Track, Technical Program Committee for NANO-NET, IEE Proc. Circuits, Devices & Systems, International Journal for Circuits, Systems and Signal Processing – NAUN.

MEMBERSHIPS OF SCIENTIFIC SOCIETIES
1. IACR (International Association for Cryptographic Research)
2. IEEE Computer Society
3. IEEE Information Theory Society
4. ACM Special Interest Group on Security, Audit and Control (SIGSAC)
5. IEEE Emerging Technologies Committee: Nano-Scale, Molecular, and Quantum Networking

The total number of publications during the career: >170

List of ten publications, from the last ten years:

1. **Gligoroski, Danilo**; Samardjiska, Simona. "Semantic Security and Key-Privacy With Random Split of St-Gen Codes", *Springer Lecture Notes in Computer Science 2016, Volume 9708,* ISBN 978-3-319-40189-8.
2. Katina Kralevska; **Danilo Gligoroski**; Harald Øverby. "General Sub-packetized Access-Optimal Regenerating Codes", *IEEE Communications Letters, Volume* 20, *Issue 6, 2016.*
3. **Danilo Gligoroski**; Katina Kralevska; Harald Øverby. "Minimal header overhead for random linear network coding", *Proceedings of IEEE International Conference on Communication Workshop (ICCW), 2015*, p. 680 – 685.
4. Simona Samardjiska; **Danilo Gligoroski**. "Approaching maximum embedding efficiency on small covers using Staircase-Generator codes", *Proceedings of IEEE International Symposium on Information Theory (ISIT), 2015*, p. 2752 – 2756.
5. **Gligoroski, Danilo**; Mihajloska, Hristina; Samardjiska, Simona; Jacobsen, Håkon; Jensen, Rune Erlend; El-Hadedy, Mohamed. "Pi-Cipher: Authenticated Encryption for Big Data", *Secure IT Systems; NordSec 2014, Springer Lecture Notes in Computer Science 2014, Volume 8788,* ISBN 978-3-319-11599-3. p. 110-128.
6. Chen, Yanling; Niemenmaa, Markku; Han Vinck, A. J.; **Gligoroski, Danilo**. "On the Error Detection Capability of One Check Digit", *IEEE Transactions on Information Theory 2013,* Volume 60.(1) p. 261-270.
7. Chen, Yanling; **Gligoroski, Danilo**; Knapskog, Svein Johan. "On a special class of multivariate quadratic quasigroups (MQQs)". *Journal of Mathematical Cryptology* 2013, Volume 7.(2) p. 111-141.
8. Kralevska, Katina; **Gligoroski, Danilo**; Øverby, Harald. "Balanced XOR-ed Coding", *Springer Lecture Notes in Computer Science* 2013, Volume 8115. p. 161-172.
9. Samardjiska, Simona; Chen, Yanling; **Gligoroski, Danilo**. "Algorithms for construction of multivariate quadratic quasigroups (MQQs) and their parastrophe operations in arbitrary Galois fields", *Journal of Information Assurance and Security* 2012.
10. Samardjiska, Simona; **Gligoroski, Danilo**. "Left MQQs whose left parastrophe is also quadratic", *Journal Commentationes Mathematicae Universitatis Carolinae* 2012 ; Volume 53.(3) p. 397-421.

Granted patent(s):   4 (+2 pending)

Invited presentations to peer-reviewed, internationally established conferences and/or international advanced schools:
1. *"Semantic Security and Key-Privacy With Random Split of St-Gen Codes"*, Pursuit of the Universal, 12th Conference on Computability in Europe, CiE 2016, Paris, France.
2. *"Security issues of HTTP/2.0", The 15th International Conference on Information Security IS2, 2014, Prague, Czech Republic.*
3. *"Cryptographic hash functions"*, NISNet - Winter School 2010, Finse, Norway.
4. *"Swiss army knife in cryptography and information security - cryptographic hash functions"*, EUNICE 2010 , Trondheim, Norway.
5. *"Why narrow-pipe cryptographic hash functions are not a match to wide-pipe cryptographic hash functions?"*, WORKSHOP ON CRYPTOGRAPHY AND SECURITY, 2010, Bergen, Norway.
6. *"Why narrow-pipe cryptographic hash functions are not a match to wide-pipe cryptographic hash functions?"*, SantaCrypt 2010, Prague, Czech Republic.
7. *"Swiss army knife in cryptography and information security - cryptographic hash functions"*, MASSEE International Congress on Mathematics - MICOM 2009.

Leadership in industrial innovation or design
2015   FORNY2020 - OptiStore, Commercialising of Patents PCT/EP2014/063315, GB1411503.4, US14/707211 and GB1507934.6, 4.2 MNOK
2015   Co-founder of NTNU-TTO Spin-off company OptiStore AS
2013   FORNY2020 - OptiNet, Commercialising of Patents PCT/EP2014/063315, GB1411503.4, 2.5 MNOK
2013   NTNU Discovery, for Patents PCT/EP2014/063315 and GB1411503.4, 1.1 MNOK
2013   Brukerstyrt Regional Innovasjonsarena (BRIA), 0.5 MNOK