Chalmers University of Technology,
Department of Computer Science and Engineering,
Rännvägen 6B (Office No 5111A),
SE-412 96, Göteborg, Sweden

email: aikmitr@chalmers.se
Phone: +46 31 772 10 40,
Webpage: http://www.cse.chalmers.se/~aikmitr/

Aikaterini Mitrokotsa

Curriculum Vitae

Education - Titles

May 2014: **Docent in Computer Science**, (corresp. of habilitation) Department of Computer Science and Engineering, Chalmers University of Technology.

02.2002-11.2007: **PhD in Computer Science**, University of Piraeus, Greece, on the Subject: **"Intrusion Detection in Computer Networks Using Machine Learning Algorithms".** Supervisor: Professor Christos Douligeris

1997-2001: **B.Sc. Degree in Computer Science**, University of Piraeus, Greece.

Working Experience

May-September 2015: (tentative period – invited period April-Sept. 2015) Invited *Visitor Associate Professor*, **Tokyo Institute of Technology**, Department of Mathematical and Computing Sciences, Tokyo, Japan.

08.2013 - Today: Assistant Professor (Docent), **Chalmers University of Technology**, Department of Computer Science & Engineering, Gothenburg, Sweden.

09.2012 - 08.2013: **Professor, University of Applied Sciences Western Switzerland** (HES-SO), School of Business Administration Geneva, Switzerland.

07.2010 - 11.2012: Senior Researcher-**Marie Curie Fellow**, **EPFL**, School of Computer & Comm. Sciences.

10.2008- 04.2010: Postdoctoral Researcher, **TU Delft**, Faculty of Elect. Eng. Math. & Comp. Science (EEMCS).

09.2007-09.2008: Visitor Assistant Professor, **Vrije Universiteit**, Dept. of Computer Science, Amsterdam, NL.

06.2002-07.2007: Visiting Faculty in the Technological Education Institute (TEI) of Chalkida, Evia, Greece.

02.2002-09.2007: Research and teaching assistant, University of Piraeus Research Center, Greece.

01.2004-03.2004: Research assistant of Hellenic Authority for the Information and Communication Security and Privacy (ADAE), Greece.

01.2002-05.2002: Consultant of Information Security for the Company Encode S.A., Greece.

Awards & Grants (as PI)

2015-2017 MoRE Mobility for Regional Excellence grant to be visitor professor at ETH Zurich (Västra Götaland Region, EU FP7) ($\sim$ 170,100 Euro).

Nov. 2014: I have received the **Computer Journal Wilkes Award for 2014** for the paper "On Selecting the nonce Length in distance-bounding Protocols". The paper is co-authored with Pedro Peris-Lopez, Christos Dimitrakakis and Serge Vaudenay.

2015-2019: **Swedish Research Council-VR (Vetenskaprådet) project grant (Unga forskare):** *PRECIS: Privacy and Security in Wearable Computing Devices* ($\sim$ 3,640,000 SEK) (very competitive success rate $< 9\%$).

2015: **Quality funding** from Chalmers for *improvement of the Cryptography course* (90,000 SEK).

2014: Funding from the D.- program of Chalmers for *improvement of the Cryptography course* (28,000 SEK).

2015-2018: **SNSF Sinergia project:** *SwissSenseSynergy* Swiss National Science Foundation ($\sim$ 1,100,000 CHF - 4 partners)

2014-2015: **Intel grant for Curriculum development:** *Learning, Security and Privacy* ($\sim$ 35,000 USD)

2014-2018: **EU Cost Action CRYPTACUS:** *CRYPTAnalysis of ubiquitous Computing Systems*

2014-2015: **STINT (Initiation grant):** Cross-layer authentication for wireless networks ($\sim$150,000 SEK - 2 partners)

2013-2017: **Chalmers ICT Areas of Advance** funding of research for 4 years (including funding for 1 PhD student) ($\sim$900.000 Euro). Very competitive (1 selected from $\sim$63).

2012-2016: **BEAT (FP7-STREP):** Biometrics Evaluation & Testing. ($\sim$3,500,000 EUR - 10 Partners).

07.2010-07.2012: **Marie Curie Intra European Fellowship (IEF)** (very competitive success rate $< 15\%$). Project Title: "PPIDR: Privacy-Preserving Intrusion Detection and Response in Wireless Communications". Funding of research for 2 years ($\sim$ 166,000 EUR)

10.2009-03.2010: **ICT Talent Grant** awarded by the TU Delft, Faculty of Electrical Engineering, Mathematics and Computer Science & the ICT Delft Research Centre.
Title of the project: "Intrusion Detection & Response in Wireless Communication".
Funding of research for 6 months ($\sim$ 35,000 EUR).

2008-2009: **NWO Rubicon Grant** awarded by the Netherlands Organization for Scientific Research,
Title of the project: "Intrusion Detection in Ubiquitous Computing Technologies".
Funding of research for 1 year (55,000 EUR).

2002-2005: Scholarship by the **Foundation of Bodossaki** for PhD studies.

2001: Led the graduation oath for the **highest GPA among all students** at the Department.

1998, 1999, 2000: Award by the **University of Piraeus** for the best performance in undergraduate studies.

1997, 1998, 1999: Best Student Award by the **National Scholarship Foundation of Greece** of undergraduate studies.

1997, 1998, 1999: Scholarship by the **National Scholarship Foundation of Greece** for undergraduate studies.

Grants (as co-PI)

2015-2019: **VR (Vetenskaprådet) project grant):** *DecentLP: Robust Decentralised Location Privacy* ($\sim$ 3,840,000 SEK), PI: Prof. Andrei Sabelfeld.

2015-2018: **H2020 EU project:** *SHARCS: on end-to-end security of ICT systems* ($\sim$ 3,100,000 Euros for all partners), PI: Assistant Professor Ioannis Sourdis.

Impact

Publications	more than 60 publications. These include top-ranked venues in information security, cryptography and communication networks.
Citations	970+, (814 in the last five years) according to Google Scholar.
h-index	15 (15 in the last 5 years) according to Google Scholar.
i10-index	22 (22 in the last 5 years) according to Google Scholar.

Languages

Greek:	Mother Tongue.
English:	Cambridge Certificate of Proficiency in English, Michigan Certificate of Proficiency in English.
French:	Certificat de Langue Français, Level C1.
Swedish:	Basic Level.
German:	Level A1.
Dutch:	Basic Level.

Professional Activities

Editorial Board

2013 - Today:	IEEE Communications Letters.
2013 - Today:	Computers & Security, Elsevier.
2015 - Today:	Ad hoc Networks, Elsevier.
2013 - Today:	KSII Transactions on Internet & Information Systems.
2012 - Today:	Information Security Journal (Taylor & Francis).

Guest Editor

2015:	Special Issue in Computer Networks, Elsevier.
2012:	Special Issue in IEEE Transactions on Dependable & Secure Computing.
2011:	Special Issue in Journal of Personal & Ubiquitous Computing, Springer.
2011:	Special Issue in Journal of Networks & Computer Applications.

Group of Experts

2014- 2019:	Management Committee (for Sweden) for the ICT Cost Action IC1403 **"Cryptanalysis of ubiquitous computing systems (CRYPTACUS)"**. Serving also as chair of the policy enforcement committee for the action.
2014- 2019:	Management Committee (Substitute MC for Sweden) for the ICT Cost Action IC1306 **"Cryptography for Secure Digital Interaction"**
2012 - 2017:	**ENISA Permanent Stakeholders' Group (PSG)** (2012-2017).
2014 - Today:	Associate Member of the Network of Excellence (EU FP7) **SysSec** (Systems Security).
2009 - 2010:	ENISA's expert group *Priorities of Research on Current & Emerging Network Technologies (PROCENT-EG) & Experts for Identifying Emerging and Future Risks Posed by New ICTs.*
2013 - Today:	**Member of WG 3** on *Secure ICT research & innovation for the Network & Information Security (NIS) platform.*
2012 - Today:	**Member of the ERCIM Working Group** in Security & Trust Management.

Conference - Workshop Organisation

2015:	STINT Workshop on Advances in Cryptography and Coding 2015, Gothenburg, Sweden
2014-2015:	ACM Workshop on Artificial Intelligence and Security (AISec 2014, 2015), co-located with ACM CCS 2014-2015.
2014:	*AfricaCrypt 2012* - International Conference in Cryptology in Africa, July 2012, Morocco.
2010:	ECML/PKDD Workshop on Privacy & Security Issues in Data Mining & Machine Learning.
2009-2010:	International Workshop on RFID Technology 2009-2010.

Reviewer

Scientific Panels:

– Research Foundation Flanders (FWO), Postdoctoral Fellow Proposals.
– National Science Foundation (NSF) CAREER Proposals.
– Research Council for Natural Sciences & Engineering at the Academy of Finland.
– Discovery Grants Natural Sciences & Engineering Research, Canada.

Journals: Journal of Computer Security (IOS Press); IEEE Transactions on Information Forensics and Security; IEEE Transactions on Pattern Analysis and Machine Intelligence; IEEE Transactions on Wireless Communications; IEEE Communications Letters; Ad Hoc Networks (Elsevier), Springer Transactions on Computational Sciences); Wireless Networks, Springer; EURASIP Journal of Information Security; International Journal of Radio Frequency Identification Technology and Applications (Inderscience); Journal of Parallel Emergent & Distributed Systems, Taylor & Francis; Sensors (MDPI); Computer Communications (Elsevier); Journal of Network and Computer Applications (Elsevier); Proceedings of the IEEE; International Journal of Communication Systems (Wiley); Journal Cluster Computing (Springer);International Journal of Network Security; Informations Systems Frontiers Journal(Springer); Journal of Pervasive and Mobile Computing (Elsevier); Journal of Computers and Security (Elsevier); KSII Transactions on Internet & Information Systems; International Journal of Computer Research; Information Sciences Journal; Computer Networks Journal (Elsevier).

Conferences: IEEE ICC 2013 - Ad-hoc and Sensor Networking Symposium, AIsec2012, ICIT 2012, WISTP 2012, AsiaCCS 2012, WISTP 2011, ACNS 2011, ICIT 2010, NGWS 2009, SecureComm 2009, LISA '08, ETFA'08, ChinaCom'08, EW'08, MSWIM'07, BROADNETS'07, IPS'06, ICCCN'05, INFOCOM 2005, ICCCN'04, ICC'04

Program Committee

Conferences:

– *IEEE Conference on Computer Communication (INFOCOM 2014-2015-2016)*
– *International Conference on Applied Cryptography and Network Security (ACNS 2014)*
– *IEEE Conference on Communications and Network Security (IEEE CNS 2013-2014-2015)*
– *Workshop on the Economics of Information Security (WEIS 2014-2015)*
– *International Conference on Availability, Reliability and Security (ARES 2013-2014-2015)*
– *Annual Conference on Privacy, Security and Trust (PST 2013-2014-2015)*
– *Workshop on Privacy and Inference 2015*
– *International Workshop on Security (IWSEC 2015)*
– *ACM International Conference on Computing Frontiers 2014 (CF'2014)*
– *Nordic Conference on Secure IT Systems (NordSec 2014)*
– *International Workshop in Information Security Theory and Practice (WISTP 2013-2014)*
– *ACM Workshop on Artificial Intelligence & Security (AISec 2012-2013)* (Colloc. with CCS)
– *Workshop on RFID Security and Privacy 2013 (RFIDsec 2013)*
– *International Conference on Cryptology in India (Indocrypt 2013)*
– *Intern. Conference on Emerging Ubiquitous Systems & Pervasive Networks (EUSPN 2013)*
– *International Conference on Wireless Information Networks and Systems (WINSYS 2013)*
– *IEEE International Workshop on Advances in Sensors and Interfaces (IWASI 2013)*
– *IEEE Symposium on Computers and Communications (ISCC'13)*
– *IFIP Conference on e-Business, e-Services, e-Society (I3E 2013)*
– *International Conference in Cryptology in Africa (AfricaCrypt 2012)*
– *International RFID EURASIP Workshop 2012, 2015*
– *International Conference on Networking and Services (ICNS 2012-2013)*
– *ACM Workshop on High Performance Mobile Opportunistic Systems (HP-MOSys 2012)*
– *IEEE ICC 2011 Next Generation Networking and Internet Symposium*
– *International Conference on Next Generation Wireless Systems (NGWS 2009)*
– *International Workshop on Vehicular Commun., Networks, & Applications (VCNA 2009)*

Institutional Responsibilities

2012-2013: **Director of the Master of Advanced Studies Program:** Information Security Management Systems, University of Applied Sciences of Western Switzerland (HES-SO).

2013: **PhD Thesis examiner-reviewer:** Jonas Magazinius, Topic: *"Dynamic Enforcement of decentralized security policies"*, Chalmers, 2013.

2011: **PhD Thesis examiner-reviewer:** Luke Mirowski, Topic: *"A whole of system approach of security analysis in RFID systems using an integrated layered reference model"*, University of Tasmania, 2011.

2013: **MSc. Thesis examiner:** Z. Chen, Topic: *"The LPN Problem & algebraic methods"*, EPFL.

List of Publications

Theses

[1] A. Mitrokotsa. *Intrusion in Computer Networks Using Machine Learning Algorithms.* PhD thesis, Department of Informatics, University of Piraeus, Greece, August 2007.

[2] A. Mitrokotsa. *Security in TCP/IP Protocol.* Bachelor thesis, Department of Informatics, University of Piraeus, Greece, 2001.

Edited Books

[3] C. Dimitrakakis, A. Mitrokotsa, B. I.P. Rubinstein, Gail-Jool Ahn, *Proceedings of the 2014 ACM Workshop on Artificial Intelligence and Security (AISec 2014)*, Scottsdale, AZ, USA, November 7, 2014. ACM 2014, ISBN 978-1-4503-3153-1.

[4] A. Mitrokotsa, S. Vaudenay, *Progress in Cryptology - Africacrypt 2012, Proceedings of the 5th International Conference on Cryptology in Africa*, Ifrane, Morocco, July 10-12, 2012, Lecture Notes in Computer Science, Vol. 7374.

[5] C. Dimitrakakis, A. Gkoulalas-Divanis, A. Mitrokotsa, V.S. Verykios, Y. Saygin, *Proceedings of the 1st International ECML/PKDD Workshop on Privacy and Security Issues in Data Mining and Machine Learning (PSDML 2010)*, Vol. 6549, Lecture Notes in Artificial Intelligence, Subseries of LNCS Springer.

[6] Q.Z. Sheng, A. Mitrokotsa, S. Zeadally, Z. Maamar, *Proceedings of the 4th International Workshop on RFID Technology - Concepts, Applications, Challenges IWRT 2010*, in conjunction with ICEIS 2010, Funchal, Madeira - Portugal, 8 - 12 June 2010, SciTePress Portugal, ISBN:978-989-8425-11-9.

[7] Q.Z. Sheng, A. Mitrokotsa, S. Zeadally, Z. Maamar, *Proceedings of the 3rd International Workshop on RFID Technology - Concepts, Applications, Challenges IWRT 2009*, in conjunction with ICEIS 2009, Milan, Italy, May 2009, INSTICC Press Portugal, ISBN: 978-989-8111-94-4.

Peer Reviewed Chapters in Books

[8] A. Mitrokotsa, M. Beye, P. Peris-Lopez, Chapter: "Threats to Networked RFID Systems". In Book: Unique Radio Innovation for the 21st Century: Building Scalable and Global RFID Networks. Eds. D. Ranasinghe, M. Sheng, S. Zeadally. Springer-Verlag., 2011, ISBN: 978-3-642-03461-9.

[9] A. Mitrokotsa and C. Douligeris. Chapter: "Integrated RFID and Sensor Networks: Architectures and Applications", In Book: *RFID and Sensor Networks: Architectures, Protocols, Security and Integrations.* Wireless Networks and Mobile Communication Series, pages 511–535. Auerbach Publications, CRC Press, Taylor and Francis Group, LLC 2010, ISBN: 978-1-4200-4288-7.

[10] A. Mitrokotsa and T. Karygiannis. Chapter: "Intrusion Detection Techniques in Sensor Networks", In Book: *Wireless Sensor Network Security*, pages 251–272. Cryptology and Information Security Series. IOS Press, 2008.

[11] A. Mitrokotsa and C. Douligeris. Chapter: "Denial of Service Attacks" In Book: *Network Security: Current Status and Future Directions*, pages 117–134. John Wiley and Sons. John Wiley and Sons, June 2007.

[12] A. Mitrokotsa and C. Douligeris. Chapter: "DoS Attacks and E-Government", In Book: *Secure eGovernment Web Services*, pages 124–142. Idea Group Publishing, Hershey PA, USA, 2007.
reprinted in:
Information Security and Ethics: Concepts, Methodologies, Tools, and Applications, Information Science Reference, 2008, IGI Global.

In International Journals after Full Peer Review

[13] C. Dimitrakakis, A. Mitrokotsa, S. Vaudenay, "Expected loss analysis for authentication in constrained channels", *Journal of Computer Security*, doi: 10.3233/JCS-140521, 2015.

[14] I. Boureanu, A. Mitrokotsa, S. Vaudenay, "Practical & Provably Secure Distance Bounding", *Journal of Computer Security*, doi: 10.3233/JCS-140518, 2015.

[15] C. Dimitrakakis, A. Mitrokotsa, "Distance Bounding Protocols: Are you Close Enough?", *IEEE Security & Privacy*, July/August 2015.

[16] A. Mitrokotsa, C. Onete, S. Vaudenay, "Location Leakage in Distance-Bounding: Why Location Privacy does not Work", *Computers & Security*, Elsevier, Vol. 45, pp. 199-209, 2014. doi: 10.1016/j.cose.2014.06.001.

[17] A. Mitrokotsa, P. Peris-Lopez, C. Dimitrakakis, S. Vaudenay. "On selecting the nonce length in distance-bounding protocols", *Computer Journal (Oxford University Press)*. 56(10): 1216-1227, (2013) doi: 10.1093/comjnl/bxt033. (**Received the Wilkes Award - Best paper in a volume of the Computer Journal**)

[18] S. Pastrana, A. Mitrokotsa, A. Orfila, P. Peris-Lopez. "Evaluation of Classification Algorithms for Intrusion Detection in MANETs". Knowledge-Based Systems, Elsevier, doi: 10.1016/j.knosys.2012.06.016, Vol. 36, December 2012, pages 217-225.

[19] A. Mitrokotsa, C. Dimitrakakis, "Intrusion Detection in MANET using Classification Algorithms: The Effects of Cost and Model Selection", *Ad hoc Networks*, Elsevier, doi: 10.1016/j.adhoc.2012.05.006. 11(1): 226–237, January 2013.

[20] P. Peris-Lopez, A. Orfila, A. Mitrokotsa, J.C.A. van der Lubbe, "A Comprehensive RFID solution to enhance inpatient medication safety", *International Journal of Medical Informatics*, 80(1): 13–24, January 2011.

[21] A. Mitrokotsa, C. Dimitrakakis, P. Peris-Lopez, J.C. Hernandez-Castro. "Reid et al.'s Distance Bounding Protocol and Mafia Fraud Attacks over Noisy Channels". *IEEE Communications Letters*, February 2010, 14(2):121–123, February 2010.

[22] A. Mitrokotsa, N. Komninos, and C. Douligeris. "Protection of an Intrusion Detection Engine with Watermarking in Ad Hoc Networks". *International Journal of Network Security*, 10(2): 93–106, March 2010.

[23] A. Mitrokotsa, M.R. Rieback, and A.S. Tanenbaum. "Classifying RFID Attacks and Defenses". *Special Issue on Advances in RFID Technology, Information Systems Frontiers, Springer*, Springer Science & Business Media, LLC 2009, 12(5):491–505, 2010.

[24] A. Mitrokotsa, N. Komninos, C. Douligeris, (2007), "Intrusion Detection and Response in Ad hoc Networks", *International Journal on Computer Research, Special Issue on Advances in Ad Hoc Network Security*, Nova Science Publishing Inc., Vol. 15, Issue 1, pages 23–55, 2007.

[25] A. Mitrokotsa and C. Douligeris. "DDoS Attacks and Defense Mechanisms: Classification and State-of-the-art". *Computer Networks*, 44(5):643–666, 5 April 2004.

In International Conferences & Workshops after Full Peer Review

[26] E. Pagnin, A. Yang, G. Hancke, A. Mitrokotsa, "Short: HB^+DB Mitigating Man-in-the-Middle attacks against HB^+ with Distance Bounding". In *Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec 2015)*, 22-26 June 2015, New York, NY USA 2015.

[27] E. Pagnin, C. Dimitrakakis, A. Abidin, A. Mitrokotsa, "On the Leakage of Information in Biometric Authentication". In *Proceedings of Indocrypt 2014*, New Delhi, India, December 2014, LNCS 8885, pp. 265-280, Springer.

[28] C. Dimitrakakis, B. Nelson, A. Mitrokotsa, B.I.R. Rubinstein, "Robust and private Bayesian inference". In *Proceedings of the International Conference on Algorithmic Learning Theory (ALT 2014)*, Bled, Slovenia, October 2014, LNCS 8776, pp. 291-305, Springer.

[29] A. Abidin, A. Mitrokotsa, "Security aspects of privacy-preserving biometric authentication based on ideal lattices and ring-LWE". In *Proceedings of the IEEE Workshop on Information Forensics and Security (WIFS 2014)*, Atlanta, USA, December 2014.

[30] A. Abidin, K. Matsuura, A. Mitrokotsa, "Security of a Privacy-Preserving Biometric Authentication Protocol Revisited", In *Proceedings of the 13th International Conference on Cryptology and Network Security (CANS 2014)*, October 2014, Heraklion, Greece, LNCS 8813, pp. 290–304, Springer.

[31] A. Mitrokotsa, "Authentication in Constrained Settings", In *Proceedings of BalkanCryptSec 2014*, October 2014, Istanbul, LNCS, Springer.

[32] A. Abidin, E. Pagnin, A. Mitrokotsa, "Attacks on Privacy-Preserving Biometric Authentication", In *Proceedings of NordSec 2014*, October 2014, Tromso, Norway, LNCS 8788, pp. 293-294, Springer.

[33] C. Dimitrakakis, B. Nelson, A. Mitrokotsa, B. Rubinstein, "Differential Privacy and Private Bayesian Inferences", In *Proceedings of NordSec 2014*, October 2014, Tromso, Norway, LNCS 8788, pp. 289-290, Springer.

[34] A. Abidin, A. Mitrokotsa, "A Privacy-preserving Biometric Authentication Protocol Revisited", In *Proceedings of YACC 2014*, Porquerolles island, France, June 2014.

[35] I. Boureanu, A. Mitrokotsa, and S. Vaudenay, "Practical & Provably Secure Distance-Bounding", In *Proceedings of the 16th Information Security Conference*, Dallas, Texas, USA, 13-15 November 2013.

[36] C. Dimitrakakis, A. Mitrokotsa, and S. Vaudenay, "Expected loss bounds for authentication in constrained channels", In *Proceedings of INFOCOM 2012*, Orlando Florida 2012, 25-30 March 2012.

[37] I. Boureanu, A. Mitrokotsa, and S. Vaudenay, "Secure & Lightweight Distance-Bounding", In Proceedings of the 2nd International Workshop on Lightweight Cryptography for Security & Privacy (LightSec 2013), 6-7 May 2013, Gebze, Turkey, LNCS 8162, pp. 97–113, Springer.

[38] I. Boureanu, A. Mitrokotsa, and S. Vaudenay, "On the Need for Secure Distance-Bounding", Extended abstract, In Proceedings of the Early Symmetric Crypto (ESC 2013) seminar, 14–18 January 2013, Mondorf-les Bains, Luxembourg.

[39] I. Boureanu, A. Mitrokotsa, and S. Vaudenay, "Towards Secure Distance Bounding", In Proceedings of the 20th International Workshop on Fast Software Encryption (FSE 2013), 11–13 March 2013, Singapore, pp. 55–67, LNCS, Vol. 8424, Springer.

[40] I. Boureanu, A. Mitrokotsa, and S. Vaudenay, "On the Pseudorandom Function Assumption in (Secure) Distance-Bounding Protocols - PRF-ness alone Does Not Stop the Frauds!", In *Proceedings of LATINCRYPT 2012, 2nd International Conference on Cryptology and Information Security in Latin America*, Santiago, Chile, October 7-10, 2012, pp. 100-120, LNCS 7533 Springer.

[41] A. Bay, I. Boureanu, A. Mitrokotsa, I. Spulber, S. Vaudenay, "The Bussard-Bagga and Other Distance Bounding Protocols under Man-in-the-Middle Attacks", In *Proceedings of Inscrypt'2012, 8th China International Conference on Information Security and Cryptology*, Nov. 28- Dec. 1, 2012, Beijing, China.

[42] C. Dimitrakakis, A. Mitrokotsa, "Near-Optimal Node Blacklisting in Adversarial Networks", 2012 Conference on Decision and Game Theory for Security (GameSec 2012), Poster Session, Budapest, Hungary, November 2012.

[43] A. Mitrokotsa, C. Onete and S. Vaudenay, "Mafia Fraud Attack against the RC distance-Bounding Protocol", In *Proceedings of the 2012 IEEE RFID Technology and Applications (IEEE RFID T-A)*, November 2012, Nice, France, pages 74-79, IEEE Press.

[44] M. Safkhani, N. Bagheri, A. Mitrokotsa, P. Peris-Lopez, "On the Traceability of Tags in SUAP RFID Authentication Protocols", In *Proceedings of the 2012 IEEE RFID Technology and Applications (IEEE RFID T-A)*, November 2012, Nice, France, pages 80-84, IEEE Press.

[45] M. Safkhani, N. Bagheri, P. Peris-Lopez, A. Mitrokotsa, J.C. Hernandez-Castro, "Weaknesses in another Gen2-Based RFID Authentication Protocol", In *Proceedings of the 2012 IEEE RFID Technology and Applications (IEEE RFID T-A)*, November 2012, Nice, France, pages 292-296, IEEE Press.

[46] J.-P. Aumasson, A. Mitrokotsa, P. Peris-Lopez, "A Note on a Privacy-Preserving Distance Bounding Protocol", In *Proceedings of the 13th International Conference on Information and Communication Security (ICICS 2011)*, 23-26 November, Beijng China. Springer Vol. 7043, pp. 78-92.

[47] J.-P. Aumasson, A. Mitrokotsa, P. Peris-Lopez, "Cryptanalysis of a Privacy-preserving Distance Bounding Protocol", In *Proceedings of the International Conference on Applications of Cryptography and Network Security (ACNS 2011)*, Industrial Track, Madeira, Spain, June 2011.

[48] P. Darcy, B. Stantic, A. Mitrokotsa, A. Sattar, "Detecting Intrusions within RFID Systems through Non-Monotonic Reasoning Cleaning", In *Proceedings of the 6th International Conference on Intelligent Sensors, Sensor Networks and Information Processing*, 7-10 December 2010, Brisbane, Australia.

[49] C. Dimitrakakis and A. Mitrokotsa. "Statistical Decision Making for Authentication and Intrusion Detection", In *Proceedings of the 8th IEEE International Conference on Machine Learning and Applications (ICMLA 2009)*, Miami, FL, USA, 13-15 December 2009, pp. 409-414, IEEE Computer Society.

[50] A. Mitrokotsa, M.R. Rieback, and A.S. Tanenbaum. "Classification of RFID Attacks". In *Proceedings of the 2nd International Workshop on RFID Technology - Concepts, Applications, Challenges (IWRT 2008), in conjunction 10th International Conference on Enterprise Information Systems*, pages 73–86, Barcelona, Spain, June 2008. INSTICC Press, Portugal.

[51] A. Mitrokotsa, M. Tsagkaris, and C. Douligeris. "Intrusion Detection in Mobile Ad Hoc Networks Using Classification Algorithms". In *Proceedings of the Seventh Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net 2008) - Advances in Ad Hoc Networking*, Computer Science, pages 133–144, Palma de Mallorca, Spain, 23-27 June 2008. Springer.

[52] A. Mitrokotsa, C. Dimitrakakis, and C. Douligeris. "Intrusion Detection Using Cost-Sensitive Classification". In *Proceedings of the 3rd European Conference on Computer Network Defense (EC2ND 2007)*, LNEE (Lecture Notes in Electrical Engineering, pages 35–46, Heraklion, Crete, Greece, 4-5 October 2007. Springer-Verlag.

[53] A. Mitrokotsa, N. Komninos, and C. Douligeris. "Intrusion Detection with Neural Networks and Watermarking Techniques for MANET". In *Proceedings of IEEE International Conference on Pervasive Services 2007 (ICPS 2007)*, pages 118–127, Instabul, Turkey, July 2007.

[54] A. Mitrokotsa, N. Komninos, and C. Douligeris. "Towards an Effective Intrusion Response Engine Combined with Intrusion Detection in Ad Hoc Networks". In *Proceedings of the 6th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net 2007)*, pages 137–144, Corfu, Greece, June 2007.

[55] A. Mitrokotsa, R. Mavropodi, and C. Douligeris. "Detecting Packet Dropping Attacks Using Emergent Self-Organizing Maps in Mobile Ad Hoc Networks". In *Proceedings of International Conference on Intelligent Systems and Computing: Theory and Applications*, pages 111–118, Ayia Napa, Cyprus, 6-7 July 2006.

[56] A. Mitrokotsa and C. Douligeris. "Intrusion Detection Using Emergent Self-Organizing Maps". In G. Antoniou et al., editor, *SETN 2006*, volume 3955 of *Lecture Notes in Artificial Intelligence*, pages 559–562, Heraklion, Greece, May 2006, Springer-Verlag.

[57] A. Mitrokotsa and C. Douligeris. "Detecting Denial of Service attacks using Emergent Self-Organizing Maps". In *Proceedings of IEEE International Symposium on Signal Processing and Information Technology (ISSPIT 2005)*, pages 375–380, Athens, Greece, December 2005.

[58] A. Mitrokotsa and C. Douligeris. "DDoS Attacks and Defense Mechanisms: A Classification". In *Proceedings of IEEE International Symposium on Signal Processing and Information Technology (ISSPIT 2003)*, pages 190–193, Darmstadt, Germany, 14-17 December 2003.

Technical Reports

[59] C. Dimitrakakis and A. Mitrokotsa, "Statistical Decision Making for Authentication and Intrusion Detection", *IAS Technical Report IAS-UVA-09-03*, April 2009.

[60] C. Dimitrakakis, B. Nelson, A. Mitrokotsa and B. I.P. Rubinstein, "Robust, Secure and Private Bayesian Inference", *CoRR abs/1306.1066*, 2013.

[61] I. Boureanu, A. Mitrokotsa and S. Vaudenay, "Practical & Provably Secure Distance-Bounding", *IACR Cryptology ePrint Archive 2013: 465 (2013).*

Other Publications

[62] A. Årnes, J. Aguado, E. Boschi, R. Benito Cortiñas, F. Gaudino, G. Hobgen, T. Karagiannis, A. Mitrokotsa, I. Naumann, P. Papadimitratos, M. Papadopouli, G. Roussos, and K. Tsakona, "Mobile Identity Management", *ENISA Position Paper*, 13 April 2010.

[63] I. Askoxylakis, P. Belimpasakis, M. Broda, L. Buttyan, S. Gorniak, S. Hoemstra de Grot, S. Ioannidis, P. Kijewski, A. Merle, A. Mitrokotsa, A. Munro, O. Popov, C.W. Probst M. Rohr, L. Romano, C. Siaterlis, C. Vishik, S. Zanero, "Priorities of Research on Current & Emerging Network Technologies", *ENISA Position Paper*, 20 April 2010.

Memberships

– Institute of Electrical and Electronic Engineers (IEEE).
– Association for Computing Machinery (ACM).
– International Association for Cryptologic Research (IACR).
– European Association of Biometrics (EAB).
– Award co-chairs for Networking Networking Women (ACM SIGMOBILE program).

Selected Invited Lectures

2015: *"RFID Security & Privacy"*, Invited Speaker RFID EURASIP Workshop 2015, Oct. 2015.

2014: *"Authentication in Constrained Settings"*, Invited Speaker BalkanCryptSec 2014, Oct. 2014.

2014: *"Distance-Bounding Protocols: Are you Close Enough?"*, Institute for Infocomm Research, Infocomm Security (ICS) Department, Singapore, Oct. 2014.

2014: *"Distance-Bounding protocols: Challenges and Directions"*, University of Tokyo, Department of Industrial Informatics, July 2014.

2014: *"Security and Privacy Challenges in Wireless Communications "*, Tokyo Institute of Technology, Department of Mathematics and Computer Sciences, July 2014.

2014: *"Security and Privacy issues in Ubiquitous Computing"*, City Univ. of Hong Kong, Dep. of Computer Science, June 2014.

2014: *"Authentication in constrained settings"*, Chinese University of Hong Kong, Institute of Theoretical Computer Science and Communications, June 2014.

2013: *"Challenges in Wireless Communications: Authentication in Constrained Settings"*, Carlos III University of Madrid, Department of Computer Science and Engineering, June 2013.

2013: *"Challenges in Wireless Communications: Authentication in Constrained Settings"*, University of Bern, Instit. of Computer Science & Applied Mathematics, Communication & Distributed Systems group, April 2013.

2013: *"Machine Learning & Security"*, University of Geneva, Computer Science Centre (CUI, Centre Universitaire d'Informatique), Machine Learning group, March 2013.

2013: *"Privacy Preserving Biometrics"*, European Biometrics Symposium 2013, Brussels, Feb. 2013.

2013: *"Authentication in Constrained Settings",* ETH Zurich, Department of Information Technology and Electrical Engineering, Communication Systems Group, Computer Engineering and Networks Laboratory, Jan. 2013.

2012: *"Distance-Bounding Protocols Challenges and Directions"*, Katholieke Universiteit Leuven (KU Leuven), Computer Security and Industrial Cryptography (COSIC), Nov. 2012.

2012: *"Near-Optimal Node Blacklisting in Adversarial Networks"*, Perspectives Workshop: Machine Learning Methods for Computer Security, Schloss Dagstuhl, Sept. 2012.

2012: *"Distance Bounding Protocols"*. International Conference on Security of Internet of Things (SecurIT 2012), Kerala, India, Aug. 2012.

2010: *"Security Challenges in RFID Communication"*. In the 3rd International EURASIP Workshop on RFID Technology, La Manga del Mar Menor, Cartagena, Spain, Sept. 2010.

2009: *"Intrusion Detection in Ubiquitous Computing Technologies"*. EPFL, School of Computer and Communication Sciences, Security and Cryptography Laboratory (LASEC), Lausanne, Switzerland, Feb. 2009.

2009: *"Security & Privacy in RFID Systems"*, invited by the European Patent Office (EPO), The Hague, the Netherlands, Sept. 2009.

2005: *"Intrusion Detection and Response in Ad Hoc Networks"*, 12th Workshop of Security: Applications, Formal Aspects and Environments in the Netherlands (SAFE-NL 2007), Utrecht, The Netherlands, Dec. 2007.

2005: *"Denial of Service Attacks"*. In *Educational Seminars in Hellenic Authority for the Information and Communication Security and Privacy (ADAE)*, Athens, Greece, March 2005.

2004: *"Classification of DDoS Attacks"*. In *Workshop: Introduction to Basic Elements of e-Security*, Sofia, Bulgaria, Dec. 2004 (invited by International Telecommunication Union (ITU)).

Interviews – Talks in Public Media

2015: Talk at the International Science Festival Gothengurg, Sweden, (Vetenskapfestivalen Göteborg) *"Security and Privacy in Wireless Communications"*.

2014: Interview at ICT Areas of Advance, Chalmers University of Technology – *"Katerina Mitrokotsa makes your data more secure"*.

2010: Interview at Télévision Suisse Romande about Mobile Applications Security.

Research Visits

18–26 June 2014;
29 Sept–11 Oct. 2014: City University of Hong Kong, Department of Computer Science (Hosted by Prof. Gerhard Hancke),

26 June – 3 July 2014: Tokyo Institute of Technology, Department of Mathematics and Computing Sciences (Hosted by Prof. Keisuke Tanaka).

Research & Development Projects

2014 - 2015: (at Chalmers) Intel grant for Curriculum development: "Learning, Security and Privacy". The goal of this project is to develop a graduate level course that focuses on topics that integrate security, privacy and machine learning such as differential privacy and adversarial learning.

2015 - 2019: (at Chalmers) Swedish Research Council (VR) project: "PRECIS – Privacy and Security in Wearable Computing devices". The goal of this project is to investigate lightweight authentication mechanisms for wearable devises that provide security and privacy guarantees.

2015 - 2017: (at Chalmers & ETHZ) MoRE – Mobility for Regional Excellence project (Västra Götaland Region) for the project: "PriSecIoT – Privacy and Security for the Future Internet of Things". The goal of this project is to set a roadmap for a unified framework for a secure and privacy-preserving IoT that scales in multiple heterogeneous devices.

2015 - 2018: (at Chalmers) SNSF Sinergia project: "SwissSenseSynergy". The goal of this project is to provide a unifying framework for secure localization and privacy-preserving location-based services.

2014 - 2015: (at Chalmers) STINT Initiation grant: "Cross-layer authentication for wireless networks". This is a project that funds research visits and our goal is to explore practical security approaches for cross-layer authentication by employing mechanisms operating at the physical layer of wireless communication. (In collaboration with City University of Hong Kong).

2012 - 2016: (at EPFL & Chalmers) BEAT: "Biometrics Evaluation and Testing". The project's goal is to propose a framework of standard operational evaluations for biometric technologies. This will be achieved by (1) developing an online and open platform to transparently and independently evaluate biometric systems against validated benchmarks, (2) designing protocols and tools for vulnerability analysis, and (3) developing standardization documents for Common Criteria evaluations.

01.07.2010 - 30.06.2012: (at EPFL) Marie Curie IEF "PPIDR: Privacy-Preserving Intrusion Detection and Response in Wireless Communications". The project' s goal is to develop privacy-preserving intrusion detection and response (IDR) techniques that strike an optimal balance between the promptness of warnings, the reliability of detection and the network performance. In order to do this, we focus on privacy-preserving algorithms for sequential decision making under uncertainty.

01.10.2009 - 31.03.2009: (at TU Delft) ICT Talent grant "Intrusion Detection and Response in Wireless Communications". In this research are investigated intrusion detection and response techniques in wireless communications and more precisely wireless ad hoc networks, sensor networks and RFID systems.

01.10.2008 - 31.09.2009: (at TU Delft) NWO Rubicon (for young talented researchers) "Intrusion Detection in Ubiquitous Computing Technologies". In this research are investigated intrusion detection and response techniques in ubiquitous computing technologies and especially sensor networks and RFID systems. Focus of this research project is detecting and responding to attacks at an early stage.

01.03.2006 - 01.06.2006: (at University of Piraeus Research Center) Participation in the project of Newsphone Hellas for the development of a Defence Scheme against Sudden Incidents.

01.01.2006 - 09.2009: (at University of Piraeus Research Center) Participation in project "Advanced Security Systems and Defence of Attacks", included in the Project of Research Support (PENED) 2003 funded by the General Secretariat for Research and Technology (GSRT) of the Ministry of Development in Greece.

03.06.2004 - 31.12.2005: (at University of Piraeus Research Center) Participation in project "Support of Computer Science studies in University of Piraeus", included in Action 2.2.2 "Integration of expansion and reformation of curriculum of higher education" for the Operational Programme for Education and Initial Vocational Training (O.P. "Education").

01.01.2004 - 28.2.2006: (at University of Piraeus Research Center) Participation in the European project "Electronic and Secure Municipal Administration for European Citizens" (e-Mayor), Sixth framework program IST Priority. The aim of the project was the provision of secure, interoperable and affordable Web services for Small and Medium sized Government Organisations (SMGOs) across Europe.

01.09.2002 - 31.11.2002: (at University of Piraeus Research Center) Supervisor of Promotion Group of the official Web Site of "Go Online", Action 1: "Informational and Support Services of Small-Medium Enterprises in e-Commerce Practices". Project: GR-Net 582/17-04-2001, code: 2027607.

01.6.2002 - 31.12.2004: (at University of Piraeus Research Center) Member of Updating Group of the official Web Site of "Go Online", Action 1: "Informational and Support Services of Small-Medium Enterprises in e-Commerce Practices" Project: GR-Net 582/17-04-2001, code: 2027607.

Teaching Experience

Spring Semester 2015: Tokyo Institute of Technology, Department of Mathematical and Computing Sciences, Master Program, Lecturer for the course, *Advanced Topics in Cryptography.*

Winter Semester 2014: Chalmers University of Technology, Department of Computer Science & Engineering, Master Program, Lecturer for the course, *Cryptography.*

Winter Semester 2013: Chalmers University of Technology, Department of Computer Science & Engineering, Master Program, Lecturer for the course, *Operating Systems.*

Spring Semester 2013: University of Applied Sciences of Western Switzerland, Bachelor of Science, Business Informatics, Lecturer for the course, *Information Security.*

Winter Semester 2012: University of Applied Sciences of Western Switzerland, Master of Science in Business Administration, Lecture for the Course, *Risk Management in Information Systems.*

Winter Semester 2012: EPFL, School of Computer and Communication Sciences, given one lecture for the Bachelor Course *Network Security.*

Spring Semester 2011-2012: EPFL, School of Computer and Communication Sciences, Master Seminar Course, *Security Protocols & Applications*, Coordinator for the course for 2 semesters. Assignment of topics to students, maintenance of course's website, supervise six master students in their projects related to the course. Participation in improving the exam subjects, marking reports and presentations.

Spring Semesters 2009-2010 (2 semesters): TU Delft, Faculty of Electrical Engineering, Mathematics and Computer Science, Four Invited Lectures for the course *Cryptography & Security* (Master Program: Electrical Engineering).

02.2008 - 08.2008 (1 semester): Vrije Universiteit, Amsterdam - Lecturer for the course *Computers and Network Security* (Bachelor Program: Informatics, Multimedia & Management (IMM), Informatics, Artificial Intelligence, Master Program: Business, Mathematics and Informatics, Computer Science Parallel and Distributed Computer Systems).

09.2007 - 1.2008 (1 semester): Vrije Univeristeit, Amsterdam - Lecturer for the course *Advanced Topics in Network Security* (Master Program: Parallel and Distributed Computer Systems).

2007 - 2008 (2 semesters): Vrije Univeristeit, Amsterdam - Responsible and coordinator for the seminar course *Literature Study in Computer Science* (Master Program: Computer Science).

10.2006 - 7.2007 (2 semesters): Technological Education Institute of Chalkida, Department of Automation, visiting faculty for the course *Object Oriented Programming (C++).*

2005 - 2006 (2 semesters): University of Piraeus - Department of Statistics and Insurance Science, teaching classes of the course *Introduction to Computing.*

2003-2004-2005 (3 semesters): University of Piraeus - Department of Informatics teaching classes of the course *Web Technologies.*

10.2005 - 7.2006 (2 semesters): Technological Education Institute of Chalkida, Evia, Greece - Department of Electrical Engineering, visiting faculty for the course *Introduction to Computing.*

10.2005 - 7.2006 (2 semesters): Technological Education Institute of Chalkida, Evia, Greece - Department of Automation, visiting faculty for the course *Object Oriented Programming (C++).*

2003-2004-2005 (4 semesters): Technological Education Institute of Chalkida, Evia, Greece - Department of Automation, visiting faculty for the course *Computer Architecture.*

09.2002 - 07.2003 (2 semesters): Technological Education Institute of Chalkida, Evia, Greece - Department of Mechanical Engineering visiting faculty for the course *Structured Programming (Fortran).*

Advising

Post-doctoral Researchers

– Dr. Aysajan Abidin, 2014-205, topic: *"Privacy-preserving biometric authentication"*, Chalmers University of Technology, Department of Computer Science and Engineering.

PhD Students

– Mrs. Elena Pagnin, 2014 - Ongoing, topic: *"Authentication protocols"*, Chalmers University of Technology, Department of Computer Science and Engineering.
– Mr. Aristide Tossou, Feb 2015 - Ongoing, topic: *"Secure and private machine learning and decision making"*, Chalmers University of Technology, Department of Computer Science and Engineering (Co-supervised with Christos Dimitrakakis).
– Mr. Pablo Picazo-Sanchez, February-April 2015, *"Security & Privacy in Wide Body Area Networks"*, Carlos III University of Madrid, Department of Computer Science and Engineering, visitor at Chalmers for three months.
– Mr. Eric Yang, November 2014, *"Cross-layer authentication for wireless networks"*, City University of Hong Kong, visitor at Chalmers for one month.
– Mr. Sergio Pastrana, 2009-2010, topic: *"Intrusion Detection in MANET"*, Carlos III University of Madrid.
– Mr. Michael Beye , 2009-2010, topic: *"RFID Security & Privacy"*, TU Delft, Faculty of Electrical Engineering, Mathematics and Computer Science.

MSc. Students

– Jing Liu, MSc. Thesis: *"Verifiable Delegation of Computation"*, Chalmers University of Technology, Department of Computer Science & Engineering, Ongoing 2015.
– Tobias Tillström and Eric Hillbom MSc. Thesis: *"Applications of smart contracts and smart property utilising blockchain technology"*, Chalmers University of Technology, Department of Computer Science & Engineering, Ongoing 2015.
– Daniel Olausson, MSc. Thesis: *"Privacy-preserving biometrics"*, Chalmers University of Technology, Department of Computer Science & Engineering, April 2015.
– Christoffer Karlsson, MSc. Thesis: *"Distance-bounding – Grouping proof protocols"*, Chalmers University of Technology, Department of Computer Science & Engineering, Aug. 2014.
– André Malm and Erica Löfström, MSc. Thesis: *"Obfuscation in a white-box environment"*, Chalmers University of Technology, Department of Computer Science & Engineering, Nov. 2014.
– Iosif Spulber MSc. Project: *"Solving the Hidden Number Problem"*, EPFL, School of Computer and Communication Sciences, Aug. 2012.
– Tamas Nagy MSc. Thesis: *"Intrusion Detection in RFID Systems"*, Vrije Universiteit, Department of Computer Science, Sept. 2008.
– Despo Galataki MSc. Project: *"Intrusion Detection within a Building"*, Vrije Universiteit, Department of Computer Science, Sept. 2008.
– Atul Mehta MSc. Project: *"Intrusion Detection for Integrated WSN & RFID System"*, Vrije Universiteit, Department of Computer Science, Sept. 2008.
– Manoli Tsagkari's MSc. Thesis: *" Intrusion Detection in Mobile Ad Hoc Networks Using Machine Learning Techniques"*, University of Piraeus, Department of Computer Science, Oct. 2007.

BSc. Students

– Arvid Karlsson, Fahad Lafta Al-Khameesi Bachelor Thesis: *Privacy-preserving Biometrics"*, Chalmers University of Technology, Department of Computer Science and Engineering, June 2014.
– Zlatka Trajcheska's Internship Project: *"Providing Multiple Certificate Validation Methods"*, EPFL, School of Computer and Communication Sciences, Aug. 2012.
– Panagiotis Petasis' Bachelor Thesis: *"Intrusion Detection Systems in Wired Networks"*, University of Piraeus, Department of Computer Science, Oct. 2007.
– Dimitris Tsotsoros' Bachelor Thesis: *"Denial of Service Attacks"*, University of Piraeus, Department of Computer Science, Oct. 2006.
– Kali Trachana's Bachelor Thesis: *"Information and Computer Network Security"*, University of Piraeus, Department of Computer Science, Feb. 2007.
– Dimitris Syrmos' Bachelor Thesis: *"Analyzing Network Traffic Using Data Mining and Fuzzy Logic"*, University of Piraeus, Department of Computer Science, Feb. 2005.
– Dimitra Papakosta's Bachelor Thesis: *"Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks"*, University of Piraeus, Department of Computer Science, June 2003.

Pedagogical Training

2014: Diploma of Higher Education, Chalmers University of Technology & University of Gothenburg
Courses Completed include:
– Supervision of Research (3 ECTS)
– Pedagogical Project (6 ECTS)
– Teaching, Learning and Evaluation (3 ECTS)
– Computers in Education (5 ECTS)

Research Interests

– Intrusion Detection & Response (Systems)
– Privacy-Preservation
– Distance Bounding Protocols
– RFID Security & Privacy
– Intrusion Response Techniques
– Denial of Service attacks
– Security in Wireless Ad hoc Networks

– Security in Sensor Networks
– Key Agreement Protocols in Mobile Ad hoc and Sensor Networks
– Future Internet
– Differential Privacy
– Privacy-preserving Biometric authentication

Research Accomplishments

I am an assistant professor at Chalmers University of Technology and the CSE department. I was recruited through a very competitive process from a program for ICT Areas of Advance that Chalmers uses to recruit international top talent and to invest in promising research directions via very competitive process (selected out of 63 candidates worldwide). Formerly, I held a position as Professor in the University of Applied Sciences of Western Switzerland (HES-SO) in Geneva, as Marie Curie IEF Fellow in EPFL as post-doctoral researcher in TU Delft and as a visitor assistant professor in Vrije Universiteit in Amsterdam.

I have recently been awarded the very prestigious grant VR unga forskare (success rate less than 9%). Moreover, I am principal investigator representing one partner (Chalmers) in the FP7 cooperation project *"BEAT: Biometric Evaluation & Testing"*, of the SNSF Sinergia project "SwissSenseSynergy" and I have received the MoRE (Mobility for Regional Excellence) grant in collaboration with ETHZ. I have been project coordinator for the Marie Curie IEF (success rate less than 15%) project *"PPIDR: Privacy-Preserving Intrusion Detection & Response"* and project leader for the project *"Intrusion Detection in Ubiquitous Computing Technologies"* a project funded from a now RUBICON research award (success rate less than 20%) that I have received in 2008. I have also been awarded the ICT talent award from TU Delft in 2009.

I was **director** of the Master of Advanced Studies program: "Information Security Management Systems" in the University of Applied Sciences of Western Switzerland (HES-SO) in Geneva (2012-2013). I am also member of ENISA (European Network of Information Security) of the permanent stakeholders group (PSG), of the Network Information Security (NIS) platform for the working group (WG3) on Secure ICT research and innovation and the ERCIM WG in Security & Trust Management.

I have written more than 60 scientific publications in international journals, books, and conference proceedings and my work has been cited almost 1000 times. I have important teaching experience and experience in supervising PhD, master and bachelor students. Among others I have taught and organised the courses *"Cryptography"*, *"Operating Systems"*, *"Computers & Networks Security"*, *"Security, Protocols and Applications"* and *"Advanced Topics in Network Security"*.

I have participated in the organisation of multiple international scientific conferences and workshops (co-chair in ACM AIsec 2014-2015, Africacrypt 2012, ECML/PKDD Workshop on Privacy & Security Issues in Data Mining & Machine Learning (PSDML'10), International Workshop on RFID Technology in 2010 and 2009 (IWRT'10, IWRT'09)). Furthermore, I have served as program committee member in major conferences in the are of information and network security and cryptography (INFOCOM 2014-2015-2016, ACNS 2014, IEEE CNS 2013-2014-2015, AI sec 2013, RFIDsec 2013, ARES 2013-2014-2015, PST 2013-2014-2015, Africacrypt 2012 and many more).

Currently, I serve as associate editor among others for the journal IEEE Communications Letters, Computers & Security (Elsevier), Ad Hoc Networks (Elsevier) and KSII Transactions on Internet & Information Systems. I was also guest editor for three special issues focusing on information security and RFID technology (for the journals IEEE Transactions on Dependable & Secure Computing, Journal of Personal & Ubiquitous Computing (Springer), Journal of Networks & Computer Applications (Elsevier)). I have also been invited multiple times to give lectures in my area of expertise by multiple organisations (European Patent Office (EPO), International Telecommunication Union (ITU)), academic institutes (ETHZ, KU Leuven, EPFL, University of Tokyo, Univ. of Bern) and international conferences and workshops (EURASIP Workshop on RFID Technology 2015, 2010, European Biometrics Symposium 2013, BalkanCryptSec 2014, Perspectives Workshop: Machine Learning Methods for Computer Security, Schloss Dagstuhl 2012).