

Antonis Michalas

Professor | Cryptographer

✉ : antonios.michalas@tuni.fi

☎ : +358 50 447-8399

🌐 : www.amichalas.com

Education

- 2009 – 2013 **PhD in Provable Security and Privacy**, *University of Aalborg*, Aalborg, Denmark.
Main Academic Interests: Network Security, Privacy, Trust, Cryptography, e-Voting, Reputation Systems, Cloud Security, Trusted Computing, Urban Sensing, Privacy, and...anything that looks interesting.
- 2006 – 2007 **Masters in Information Technology and Telecommunications**, *Athens Information Technology*, Athens, Greece.
Main Academic Interests: Computer Security, e-Learning, Web Technologies, Semantic Web.
- 2000 – 2006 **Degree in Mathematics**, *University of Crete*, Heraklion, Crete.
Main Academic Interests: Algebra, Approximation Theory, Mathematical Programming.

PhD Thesis

- Title *Trust & Privacy in Distributed Networks*
- Supervisors Professor Neeli R. Prasad & Professor Nikos Komninos
- External Collaboration During my PhD I participated in the following external activities:
- Summer School. “*Mobile systems and eHealth security*”. University of Agder, Norway, Grimstad
 - Visitor for three months at Princeton University, New Jersey, USA

Professional Experience

- 06/2025 – Current **Full Professor**, TAMPERE UNIVERSITY, DEPARTMENT COMPUTING SCIENCES.
Promoted to Full Professor.
- 12/2021 – 2025/05 **Associate Professor**, TAMPERE UNIVERSITY, DEPARTMENT COMPUTING SCIENCES.
Promoted to Associate Professor.
- 02/2018 – 12/2021 **Assistant Professor**, TAMPERE UNIVERSITY OF TECHNOLOGY, DEPARTMENT OF COMPUTING SCIENCES.
I joined the Department of Computing Sciences at Tampere University (TUNI) as an assistant professor in the beginning of 2018 (formerly known as Tampere University of Technology). At TUNI, along with [Billy Brumley](#), I co-lead the Network and Information Security group (NISEC). The group consists of PhD students, professors, and researchers who conduct research in areas spanning from the theoretical foundations of cryptography to the design and implementation of leading edge efficient and secure communication protocols. Apart from my research work at NISEC, as an assistant professor, I am actively involved in the teaching activities of the University. Finally, my role also includes student supervision and research projects coordination.

- 07/2018 – 05/2019 **Security, Privacy & GDPR Consultant**, GREEK NATIONAL DOCUMENTATION CENTER.
Responsible for the security analysis of the main IT systems that were used in the National Documentation Center as well as on the offered public services. Furthermore, my work involved the design of policies and security and privacy-preserving protocols that would make the overall organization GDPR-compliant. Finally, I was tasked with improving the security of existing systems/applications by staging attacks and providing solutions for any discovered vulnerabilities.
- 09/2015 – 02/2018 **Lecturer in Cyber Security**, UNIVERSITY OF WESTMINSTER, COMPUTER SCIENCE.
As a lecturer (assistant professor) I am teaching both undergraduate and postgraduate courses related to cryptography, forensics, cyber security and network security. My role expands to student supervision and research group coordination. In parallel, I am an active member of the department's project development and research activities. In addition to that, I am leading the cyber security research group at the University of Westminster. As the head of the cyber security research group, I lead research projects focused on network security and cryptography. The group comprises PhD students, professors and researchers. We mainly focus on applied research in security and privacy of widely deployed communication networks.
- 01/2014 – 09/2015 **Postdoctoral Researcher**, SWEDISH INSTITUTE OF COMPUTER SCIENCE (SICS).
Actively involved in the current national and European research projects in the Security Lab, where I combine research with student supervision and project management. Within one year of starting at SICS, I have successfully obtained funding for three EU projects. Currently, I conduct research in the field of Security & Privacy for People-Centric Sensing, Cloud Computing, Trusted Computing, e-Voting Systems and Secure & Privacy Preserving e-Health Systems.
- 03/2013 – 01/2014 **Security Consultant**, CYBER DEFENCE DEPARTMENT, HELLENIC ARMY.
Responsible for implementing and managing an information encryption system for the specific needs of the Hellenic Army. My work involved designing a secure single sign on protocol which connects online services of different web applications used by the military personnel. Additionally, I was tasked with improving the security of existing systems/applications by staging attacks and providing solutions for any discovered vulnerabilities.
- 2011 – 2012 **Senior Web Developer**, DPG DIGITAL MEDIA, Athens, Greece.
I was the team manager for Web-Related Projects. More precisely, I was responsible for talking directly with the clients and the Management Department in order to understand the needs of each project. Moreover, I was distributing the work to developers based on the requirements of each project while at the same time I was responsible for evaluating each part of the deliverable as well as programming the most demanding parts of the projects.
Main working environments: PHP, MYSQL, JAVASCRIPT, JQUERY, AJAX, XML, JSON
- 2009 – 2011 **Researcher**, ATHENS INFORMATION TECHNOLOGY, Athens, Greece.
Conducting research in network security. More precisely, my research focused on private and secure e-voting systems, reputation systems, privacy in decentralized environments, cloud computing and privacy preserving protocols in participatory sensing applications.
- 2008 – 2009 **Software Engineer**, I-CUBE S.A., Athens, Greece.
Development of European Union research projects.
Main working environments: MICROSOFT .NET (C#, VB), JAVASCRIPT, MYSQL, PHP, JQUERY, AJAX AND WEB SERVICES
- 2007 – 2008 **Software Engineer**, INTRALOT S.A., Athens, Greece.
Programming and development of lottery-related games in Europe, the USA and Australia.
Main working environments: MICROSOFT .NET (C#, VB), JAVASCRIPT, ORACLE, CRYSTAL REPORTS AND WEB SERVICES
- 2001 – 2004 **Web Developer**, WEBLINE S.A., Heraklion, Crete.
During my undergraduate studies I worked as a Web Developer at Weblines S.A.
Main working environments: XHTML, PHP, MYSQL, JAVASCRIPT, XML

2024 – 2027 SWARMCHESTRATE, EU HORIZON Project.

Swarmhestrate develops a novel decentralised application-level orchestrator, based on the notion of self-organised interdependent Swarms. Application microservices are managed in a dynamic Orchestration Space by decentralised Orchestration Agents, governed by distributed intelligence that provides matchmaking between application requirements and resources, and supports the dynamic self-organisation of Swarms. Knowledge and trust, essential for the operation of the Orchestration Space, is managed through blockchain-based trusted solutions using methods of Self-Sovereign Identities (SSI) and Distributed Identifiers (DID). End-to-end security of the overall system will be assured by utilising state-of-the-art cryptographic algorithms and privacy-preserving data analytics.

2022 – 2025 HARPOCRATES, EU HORIZON Project.

HARPOCRATES leverages novel cryptographic schemes to advance the capabilities of Privacy-Preserving Machine Learning (PPML), thus enabling decentralised training, validation, and prediction on encrypted data. Such privacy-preserving services and secure computation enable users to both benefit from cloud-based machine intelligence and maintain control over data.

2022 – 2026 FACILITATE, EU H2020 Project.

FACILITATE is a project built on a patient-centered, data-driven, technological platform where an innovative data sharing and re-use process allows the returning of clinical trial data to study participants within a GDPR compliant and approved ethical framework. FACILITATE starts-off by providing clear rules in a trusted ethical, legal and regulatory ecosystem before engaging patients as data generators. This avoids the current situation where clinical data are siloed in separate repositories without any possibility to be used beyond their original single-sided purpose. FACILITATE will provide the technological solutions to comply with GDPR in medical research by building on the empowered stakeholders' willingness to share and re-use their data.

2021 – 2024 ARROWSMITH, Industrial Project.

The vision of ARROWSMITH is to further the evolution of smart cities by helping the area to take off and pave the way towards development of secure and trusted deployments that will facilitate protection against a wide range of hardware and software-based attacks. Smart cities routinely gather huge amounts of data in a top-down fashion without any public review and noticeable absence of security mechanisms that should not only ensure the confidentiality and integrity of data but also, the trusted state of the IoT devices used for data capturing, processing and sharing. ARROWSMITH aims to change the security outlook in smart cities by designing a Security Framework that will be resistant to a plethora of malicious behaviours.

2019 – 2022 CYBELE, EU H2020 Project.

CYBELE generates innovation and creates value in the domain of agri-food, and its verticals in the sub-domains of PA and PLF in specific, as demonstrated by the defined real-life industrial cases, empowering capacity building within the industrial and research community. Since agriculture is a high-volume business with low operational efficiency, CYBELE aspires at demonstrating how the convergence of HPC, Big Data, Cloud Computing and the IoT can revolutionize farming, reduce scarcity and increase food supply, bringing social, economic, and environmental benefits. CYBELE intends to safeguard that stakeholders have integrated, unmediated access to a vast amount of large scale datasets of diverse types from a variety of sources, and they are capable of generating value and extracting insights, by providing secure and unmediated access to large-scale HPC infrastructures supporting data discovery, processing, combination and visualization services, solving challenges modelled as mathematical algorithms requiring high computing power.

2018 – 2021 ASCLEPIOS, EU H2020 Project.

The vision of ASCLEPIOS is to maximize and fortify the trust of users on cloud-based healthcare services by developing mechanisms for protecting both corporate and personal sensitive data. While researchers have developed many theoretical models that could enhance the security level of healthcare services, only a rudimentary set of techniques are currently in use. ASCLEPIOS is addressing these limitations by utilizing several modern cryptographic approaches to build a cloud-based eHealth framework that protects users' privacy and prevents both internal and external attacks.

2017 – 2020 CloudiFacturing, EU H2020 Project.

CloudiFacturing is bringing and progressing advanced ICT in the field of Cloud/HPC-based modelling and simulation, data analytics for online factory data, and real-time support to European manufacturing SMEs, contributing to their competitiveness and resource efficiency via optimizing production processes and producibility. CloudiFacturing demonstrates the technical and economic impact on the basis of more than 20 cross-national application experiments for first-time users of the technologies being addressed and progressed during the project. The technological innovation focus of CloudiFacturing has been chosen on the observation that real production processes in many cases differ from their virtually simulated counterparts and that online factory data – albeit being available – is hardly used to improve the simulated and real production processes.

2016 – 2019 COLA, EU H2020 Project.

The overall objective of the COLA project is that by building on and extending current research results, it will define and provide a reference implementation of a generic and pluggable framework that supports the optimal and secure deployment and run-time orchestration of cloud applications. COLA will demonstrate the applicability and impact of the solution via large scale near operational level SME and public sector pilots and demonstrators, and will also define a clear pathway how the innovation can be delivered to the market.

2015 – 2018 PaaSword, EU H2020 Project.

The vision is to fortify trust in cloud services and increase the adoption rate of cloud-based solutions. To this end, we design and develop mechanisms that safeguard both corporate and personal data for cloud infrastructures and storage services. Furthermore, by addressing major cloud security challenges, we provide essential knowledge to organizations that wish to securely migrate to the cloud. Six pilots together with EU industrial partners will be implemented.

2015 – 2016 Trusted Telecommunication IaaS Platform, EU EIT Project.

This project mainly focus on the design and implementation of data confidentiality and integrity protection mechanisms for IaaS clouds that will open up radical new telecommunication business opportunities. In particular this new business offering will allow transparent storage isolation between IaaS clients and their data. The main target for the activity is to extend the OpenStack open source project with particular focus on secure storage. In particular, one important task is to extend the previous results with novel principles for efficient data search over encrypted data (Symmetric Searchable Encryption).

2013 – 2014 InfraCloud, Swedish National Project.

InfraCloud is a Swedish project that targets the security of critical information in an infrastructure as a Service (IaaS) cloud. More precisely, InfraCloud utilizes and builds upon previous research on the verification of computer resources in public IaaS clouds and paves the way for applications and organizations that wishes to securely move to a public cloud. In addition to that, the absence of reliable data sharing mechanisms is addressed by providing a framework, which enables clients of IaaS clouds to securely share data and clearly define access rights granted to peers.

2010 – 2011 Secure Single Sign On & Identity Management, Greek National Project.

The concept of this project was to design and implement a secure Single-Sign-On (SSO) framework and Identity Management System for an international company. In a SSO approach users authenticate themselves only once and they are automatically logged into application servers as necessary without required any further interaction. For the needs of this project, I implemented the Kerberos architecture in order to secure the login procedure without sending the password over the channel as well as for securing each request from users. To do so, each *http* request was based on unique tickets with unique session keys. Thus providing an additional level of security.

2009 – 2010 **PERFORM**, *EU FP7 Project*.

The PERFORM project aims to tackle problems associated with the efficient remote health status monitoring, the qualitative and quantitative assessment and the treatment personalization for people suffering from neurodegenerative diseases and movement disorders, such as Parkinson's disease (PD). Aspires to research and develop an innovative, intelligent system for monitoring neurodegenerative disease evolution through the employment of a wide range of wearable micro-sensors, advanced knowledge processing and fusion algorithms.

2009 **I-WAY**, *EU FP7 Project*.

A Geographic Information System for a European Research program. The goal of I-WAY is to develop a multi-sensorial system that can ubiquitously monitor and recognize the psychological condition of driver as well as special conditions prevailing in the road environment.

Research Funding and Grants

2024 **DIGITAL-ECCC-2024-DEPLOY-CYBER-06-PQCINDUSTRY**.

Project Title: Post-Quantum Cryptography As-a-Service for Common Transmission Systems and Infrastructures (PiQASO).

Duration & Grant: Research funding for 3 years (509,600€/6,597,620€, 25 Partners).

Role: PI, WP Leader & Researcher.

Status: [Active](#)

2023 **H2020-CL3-2021-CS-01-04**.

Project Title: Application-Level Swarm-Based Orchestration Across the Cloud-to-Edge Continuum (SWARMCHESTRATE).

Duration & Grant: Research funding for 3 years (468,625€/5,439,558€, 14 Partners).

Role: PI, WP Leader & Researcher.

Status: [Active](#).

2022 **H2020-CL3-2021-CS-01-04**.

Project Title: Federated Data Sharing and Analysis for Social Utility (HARPOCRATES).

Duration & Grant: Research funding for 3 years (718,750€/4,408,800€, 13 Partners).

Role: PI, [Coordinator](#) & WP Leader.

Status: [Completed](#).

H2020-IMI2-2020-23-01.

Project Title: FrAmework for Clnical trlal participants daTA reutilization for a fully Transparent and Ethical ecosystem (FACILITATE).

Duration & Grant: Research funding for 4 years (215,250€/3,260,000€, 26 Partners).

Role: PI, WP Leader & Researcher.

Status: [Active](#).

2021 **Industrial Project**.

Project Title: ARROWSMITH: Living (Securely) on the Edge.

Duration & Grant: Research funding for 3 years (700,000€/1,500,000€, 3 Partners).

Role: PI, WP Leader & Researcher.

Status: [Completed](#).

2018 **H2020 SC1-FA-DTS-2018-2020**.

Project Title: Advanced Secure Cloud Encrypted Platform for Internationally Orchestrated Solutions in Healthcare (ASCLEPIOS).

Duration & Grant: Research funding for 3 years (634,650€/4,840,000€, 10 Partners).

Role: PI, [Scientific Coordinator](#) & WP Leader.

Status: [Completed](#).

H2020 ICT-11-2018-2019.

Project Title: Fostering Precision Agriculture and Livestock Farming Through Secure Access to Large-Scale HPC-Enabled Virtual Industrial Experimentation Environment Empowering Scalable Big Data Analytics (CYBELE).

Duration & Grant: Research funding for 3 years (424,375€/12,407,673€, 31 Partners).

Role: PI, WP Leader & Researcher.

Status: Completed.

2017 H2020 IND-CE-2016-17.

Project Title: Cloudification of Production Engineering for Predictive Digital Manufacturing (CloudiFacturing).

Duration & Grant: Research funding for 3.5 years (516,250€/8,712,521€, 33 Partners).

Role: WP Leader & Researcher.

Status: Completed.

2016 H2020 ICT-06-2016.

Project Title: Cloud Orchestration at the Level of Application (COLA).

Duration & Grant: Research funding for 3.5 years (809,688€/4,238,580€, 14 Partners).

Role: WP Leader & Researcher.

Status: Completed.

2015 ICT-TNG Proposal.

Project Title: Efficient Cloud-Based Privacy Preserving Mobile Sensing.

Duration & Grant: Research funding for 1 year (\approx 53,421€, Individual Funding).

Role: PI, Project Coordinator & Researcher.

Status: Completed.

2014 H2020 ICT-2014-1 Proposal.

Project Title: A Holistic Data Privacy and Security by Design Platform-as-a-Service Framework Introducing Distributed Encrypted Persistence in Cloud-based Applications (PaaSword).

Duration & Grant: Research funding for 3 years (617,750€/3,984,575€, 10 Partners).

Role: PI, Scientific Coordinator & Researcher.

Status: Completed.

European Institute of Innovation & Technology (EIT) Proposal.

Project Title: Trusted Telecommunication IaaS Platform.

Duration & Grant: Research funding for 1 year (120,000€/320,000€, 3 Partners).

Role: PI, Project Coordinator & Researcher.

Status: Completed.



Teaching - Supervising

09/2015 – Current Tampere University, University of Westminster.

As an Assistant Professor at Tampere University and the University of Westminster, I have been involved in the following undergraduate and postgraduate courses:

A. Postgraduate

- Security Protocols: Helping Alice and Bob to Share Secrets (Tampere University – Course Leader)
- Network Security (Tampere University of Technology – Course Leader)
- Internet Security (University of Westminster – Course Leader)
- Computer Security & Applications (University of Westminster – Course Leader)

B. Undergraduate

- Security & Forensics (University of Westminster – Assistant)
- Information Technology Security (University of Westminster – Course Leader)
- Algorithms and Complexity (University of Westminster – Assistant)

2009 – 2011 Athens Information Technology.

As a researcher I have been regularly involved in the provision (by giving a number of lectures and organizing lab exercises/seminars) of several courses related to security and applied cryptography.

Supervising PostDoctoral Researchers.

Bin Liu **Applied Cryptography**, 04/2021 – Current.

University: Tampere University, Tampere, Finland.

Role: Main Supervisor

Reyahneh **Blockchains and Security in Decentralized Networks**, 11/2020 – Current.

Rabbaninejad **University:** Tampere University, Tampere, Finland.

Role: Main Supervisor

Hai-Van **Cloud Security**, 02/2017 – 02/2018.

Dang **University:** University of Westminster, London, UK.

Role: Main Supervisor

Supervising PhD Students.

Mélina **Field: Applied Cryptography.**

Hadjeres **University:** Tampere University, Tampere, Finland.

Role: Main Supervisor

Status: [Expected in 2029](#)

Mindaugas **Field: Privacy-Preserving Machine Learning.**

Budzys **University:** Tampere University, Tampere, Finland.

Role: Main Supervisor

Status: [Expected in 2027](#)

Hossein **Field: Provable Security.**

Abdinasibfar **University:** Tampere University, Tampere, Finland.

Role: Main Supervisor

Status: [Expected in 2027](#)

Camille **Field: Applied Cryptography.**

Foucault **University:** Tampere University, Tampere, Finland.

Role: Main Supervisor

Status: [Expected in 2027](#)

Tanveer Khan **Advances in Privacy-Preserving Machine Learning.**

University: Tampere University, Tampere, Finland.

Role: Main Supervisor

Status: [Completed \(29.09.2025\)](#), *Opponent:* [Kaitai Liang](#)

Eugene **Modern Cryptographic Schemes on Constrained Devices.**

Frimpong **University:** Tampere University, Tampere, Finland.

Role: Main Supervisor

Status: [Completed \(07.02.2025\)](#), *Opponent:* [Vladimir A. Oleshchuk](#).

Alexandros **Hidden in the Cloud: Advanced Cryptographic Techniques for Untrusted Cloud Environments.**

Bakas **University:** Tampere University, Tampere, Finland.

Role: Main Supervisor

Status: [Completed \(15.02.2024\)](#), *Opponent:* [Rafael Dowsley](#).

Supervising MSc Students.

- **Julia Ruoranen:** Anamorphic Encryption: Theory and Applications
Tampere University, Tampere, Finland, 2025
- **Taleel Wasam:** Analysis of PQConnect - And its underlying cryptographic primitives
Tampere University, Tampere, Finland, 2025
- **Muhammad Ahmed:** Privacy vs Accuracy: Trade-offs in Federated Learning
Tampere University, Tampere, Finland, 2025
- **Asif Ibtehad:** Cross-Platform Privacy Tool for Facebook: Architecture and Implementation
Tampere University, Tampere, Finland, 2025
- **Paavo Peltopihko:** Decentralized Identities and the EU Digital Wallet.
Tampere University, Tampere, Finland, 2024
- **Yuhang Du:** Practical Obfuscation for Privacy on Social Media Platforms.
Tampere University, Tampere, Finland, 2023
- **Cecylia Borek:** Functional Encryption and Operations on Encrypted Data.
Tampere University, Tampere, Finland, 2022
- **Mindaugas Budzys:** Privacy-Preserving Machine Learning: Classifying Encrypted Data.
Tampere University of Technology, Tampere, Finland, 2022
- **Md Monirul Islam:** Implementing Attribute-Based Encryption and Symmetric Searchable Encryption in Isolated Environments.
Tampere University of Technology, Tampere, Finland, 2019
- **Nusrath Jahan Mouri:** Implementing Security Protocols on IoT Devices.
Tampere University of Technology, Tampere, Finland, 2019
- **Sutirtho Majumdar:** A Scalable Testbed for IoT Security Evaluation.
Tampere University of Technology, Tampere, Finland, 2019
- **Alexandr Zalitko:** Bypassing HSTS in Firefox
University of Westminster, London, UK, 2017
- **Eugene Frimpong** Privacy Controls in Social Media – Case Study: The Cambridge Analytica Files.
University of Westminster, London, UK, 2017
- **Inigo Ayesa:** Security in Vehicular Communication
University of Westminster, London, UK, 2017
- **Asparuh Stefanov:** Penetration Testing With Raspberry Pi 3 Micro-controllers.
University of Westminster, London, UK, 2017
- **Felipe Solferini:** The Race of Cryptocurrency.
University of Westminster, London, UK, 2016
- **Kashif Ghafoor:** Are Your Pictures Truly Yours?
University of Westminster, London, UK, 2016
- **Joolokeni Haimbala:** Secure Cloud Storage with a focus on Searchable Encryption.
University of Westminster, London, UK, 2016
- **Rohan Murray:** MemTri: A Memory Forensics Triage Tool using Bayesian Network and Volatility.
University of Westminster, London, UK, 2016

Publications

Journals 2022.

- Eugene Frimpong, **Antonis Michalas** and Amjad Ullah. “*Footsteps in the Fog: Certificateless Fog-Based Access Control*”. Journal of Computers & Security, Elsevier, 2022. [[ePrint](#)], [[Code](#)], CORE Ranking: B
- Tassos Dimitriou and **Antonis Michalas**. “*Incentivizing participation in Crowd-sensing applications through fair and private Bitcoin rewards*”. IEEE Access Journal, IEEE, 2022. [[ePrint](#)], CORE Ranking: C

2021.

- Tanveer Khan and **Antonis Michalas**. “*Seeing and Believing: Evaluating the Trustworthiness of Twitter Users*”. IEEE Access Journal, IEEE, 2021. [\[ePrint\]](#)
- Tanveer Khan, **Antonis Michalas** and Adnan Akhuzada. “*Fake News Outbreak 2021: Can We Stop the Viral Spread?*”. Journal of Network and Computer Applications, Elsevier, 2021. [\[ePrint\]](#), CORE Ranking: A

2020.

- Alexandros Bakas, Hai-Van Dang, **Antonis Michalas** and Alexandr Zalizko. “*The Cloud we Share: Access Control on Symmetrically Encrypted Data in Untrusted Clouds*”. IEEE Access Journal, IEEE, 2020. [\[ePrint\]](#), [\[Code\]](#)
- Marcela Tuler de Oliveira, Alexandros Bakas, Eugene Frimpong, Adrien E. D. Groot, Henk A. Marquering, **Antonis Michalas** and Silvia D. Olabariaga. “*A Break-Glass Protocol based on Ciphertext-Policy Attribute-Based Encryption to Access Medical Records in the Cloud*”. Annals of Telecommunications, Springer, 2020. [\[ePrint\]](#)

2017.

- Rafael Dowsley, **Antonis Michalas**, Matthias Nagel and Nicolae Paladi. “*A Survey on Design and Implementation of Protected Searchable Data in the Cloud*”. Journal of Computer Science Review, Elsevier, 2017. [\[ePrint\]](#)
- Y. Verginadis, **Antonis Michalas**, P. Gouvas, G. Schiefer, G. Hubsch and I. Paraskakis. “*PaaS-word: A Holistic Data Privacy and Security by Design Framework for Cloud Services*”. Journal of Grid Computing, a special issue on “Cloud Computing and Services Science”. Springer, 2017. [\[ePrint\]](#), CORE Ranking: B
- Kassaye Yitbarek Yigzaw, **Antonis Michalas** and Johan Gustav Bellika. “*Secure and Scalable Deduplication of Horizontally Partitioned Health Data for Privacy-Preserving Distributed Statistical Computation*”. Journal of Medical Informatics and Decision Making (BMC), 2017. [\[ePrint\]](#), CORE Ranking: B

2016.

- Nicolae Paladi, Christian Gehrmann and **Antonis Michalas**. “*Providing End-User Security Guarantees in Public Infrastructure Clouds*”. IEEE Transactions on Cloud Computing, a special issue on “Cloud Security Engineering”, IEEE, 2016. [\[ePrint\]](#)
- Kassaye Yitbarek Yigzaw, **Antonis Michalas** and Johan Gustav Bellika. “*Secure and scalable statistical computation of questionnaire data in R*”. IEEE Access Journal, a special issue of Big Data Analytics for Smart and Connected Health, IEEE, 2016. [\[ePrint\]](#)

2014.

- Tassos Dimitriou and **Antonis Michalas**. “*Multi-Party Trust Computation in Decentralized Environments in the Presence of Malicious Adversaries*”. Ad Hoc Networks Journal, a special issue on “Smart Solutions for Mobility Supported Distributed and Embedded Systems”, Elsevier, 2014. [\[ePrint\]](#)

2012.

- **Antonis Michalas**, Tassos Dimitriou, Thanassis Gianetsos, Nikos Komninos and Neeli R. Prasad. “*Vulnerabilities of Decentralized Additive Reputation Systems Regarding the Privacy of Individual Votes*”. Springer Wireless Personal Communication, Springer, 2012. [\[ePrint\]](#), CORE Ranking: C

2011.

- **Antonis Michalas**, Nikos Komninos and Neeli R. Prasad. “*Mitigate DoS and DDoS attack in Ad Hoc Networks*”. International Journal of Digital Crime and Forensics, IGI Global, 2011. [\[ePrint\]](#)

Conferences 2026.

- **Antonis Michalas** and Alexandros Bakas. “*It Runs and it Hides: A Function-Hiding Construction for Private-Key Multi-Input Functional Encryption*”. In Proceedings of the 12th International Conference on Information Systems Security and Privacy (ICISSP), Marbella, Spain, March 4–6, 2026. [\[ePrint\]](#)

2025.

- Tanveer Khan and **Antonis Michalas**. “*Oops!... They Stole it Again: Attacks on Split Learning*”. In Proceedings of the 18th ACM Workshop on Artificial Intelligence and Security (AISec), co-located with the 32nd ACM Conference on Computer and Communications Security (CCS), Taipei, Taiwan, October 17, 2025. [\[ePrint\]](#)
- Khoa Nguyen, Tanveer Khan and **Antonis Michalas**. “*A Privacy-Centric Approach: Scalable and Secure Federated Learning Enabled by Hybrid Homomorphic Encryption*”. In Proceedings of the Workshop on Responsible Machine Learning in Healthcare co-located with the European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases (ECML PKDD), Porto, Portugal, September 15–19, 2025. [\[ePrint\]](#), [\[Code\]](#)
- Tanveer Khan, Mindaugas Budzys and **Antonis Michalas**. “*Split Happens: Combating Advanced Threats with Split Learning and Function Secret Sharing*.” In Proceedings of the 13th IEEE Conference on Communications and Network Security (CNS). Avignon, France, September 8–11, 2025. [\[ePrint\]](#), [\[Code\]](#)
- Eugene Frimpong, Bin Liu, Camille Nuoskala and **Antonis Michalas**. “*Blind Brother: Attribute-Based Selective Video Encryption*”. In Proceedings of the 15th ACM Conference on Data and Application Security and Privacy (CODASPY’25), Pittsburgh, PA, USA, June 4–6, 2025. [\[ePrint\]](#)

2024.

- Reyhaneh Rabaninejad, **Antonis Michalas** and Salil Kanhere. “*Rainbow Over Clouds: A Lightweight Pairing-free Multi-Replica Multi-Cloud Public Auditing Scheme*”. In Proceedings of the 19th International Conference on Risks and Security of Internet and Systems (CRISIS’24), Aix-en-Provence, France, 26–28 November 2024 [CORE Ranking](#): C.
- Khoa Nguyen, Mindaugas Budzys, Eugene Frimpong, Tanveer Khan and **Antonis Michalas**. “*A Pervasive, Efficient and Private Future: Realizing Privacy-Preserving Machine Learning Through Hybrid Homomorphic Encryption*”. In Proceedings of the 22nd IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC’24), Boracay Island, Malay, Philippines, 5–8 November 2024. [\[ePrint\]](#), [\[Code A\]](#), [\[Code B\]](#), [CORE Ranking](#): C.
- Camille Nuoskala, Hossein Abdinasibfar and **Antonis Michalas**. “*SPADE: Digging into Selective and PArTial DEncryption using Functional Encryption*”. In Proceedings of the 20th EAI International Conference on Security and Privacy in Communication Networks (SecureComm’24), Dubai, UAE, 28–30 October 2024. [\[ePrint\]](#), [\[Code\]](#), [CORE Ranking](#): C.
- Tanveer Khan, Mindaugas Budzys, Khoa Nguyen and **Antonis Michalas**. “*Wildest Dreams: Reproducible Research in Privacy-Preserving Neural Network Training*”. In Proceedings of the 24th Privacy Enhancing Technologies Symposium (PETS’24), Bristol, U.K., 15–20 July 2024. [\[ePrint\]](#), [CORE Ranking](#): A
- Iaroslav Gridin and **Antonis Michalas**. “*Point Intervention: Improving ACVP Test Vector Generation Through Human Assisted Fuzzing*”. In Proceedings of the 26th International Conference on Information and Communications Security (ICICS’24), 26–28 August, 2024, Mytilene, Greece. [\[ePrint\]](#), [\[Code\]](#), [CORE Ranking](#): C
- Camille Foucault, Reyhaneh Rabbaninejad, Tassos Dimitriou and **Antonis Michalas**. “*FE[r]Chain: Enforcing Fairness in Blockchain Data Exchanges Through Verifiable Functional Encryption*”. In Proceedings of the 29th ACM Symposium on Access Control Models and Technologies (SACMAT), San Antonio, Texas, USA, 15–17 May, 2024. [\[ePrint\]](#), [CORE Ranking](#): C

2024.

- Tanveer Khan, Mindaugas Budzys and **Antonis Michalas**. “*Make Split, not Hijack: Preventing Feature-Space Hijacking Attacks in Split Learning*”. In Proceedings of the 29th ACM Symposium on Access Control Models and Technologies (SACMAT), San Antonio, Texas, USA, 15–17 May, 2024. [[ePrint](#)], [[Code](#)], [CORE Ranking](#): C
- Eugene Frimpong, Khoa Nguyen, Mindaugas Budzys, Tanveer Khan and **Antonis Michalas**. “*GuardML: Efficient Privacy-Preserving Machine Learning Services Through Hybrid Homomorphic Encryption*”. In Proceedings of the 39th ACM/SIGAPP Symposium On Applied Computing (SAC’24), Avila, Spain, 08–12 April 2024. [[ePrint](#)], [[Code A](#)], [[Code B](#)], [CORE Ranking](#): B
- Eugene Frimpong, Alexandros Bakas, Camille Foucault and **Antonis Michalas**. “*Need for Speed: Leveraging the Power of Functional Encryption for Resource-Constrained Devices*”. In Proceedings of the 9th International Conference on IoT, BigData and Security (IoTBDs’24), Angers, France, 28–30 April 2024. [[ePrint](#)], [[Code](#)], [CORE Ranking](#): C
- Tanveer Khan, Fahad Sohrab, **Antonis Michalas** and Moncef Gabbouj. “*Trustworthiness of X Users: A One-Class Classification Approach*”. In Proceedings of the 38th International Conference on Advanced Information Networking and Applications (AINA-2024), Kitakyushu, Japan, 19–17 April 2024. [[ePrint](#)], [[Code](#)], [CORE Ranking](#): B

2023.

- Tanveer Khan, Khoa Nguyen and **Antonis Michalas**. “*A More Secure Split: Enhancing the Security of Privacy-Preserving Split Learning*”. In Proceedings of the 28th Nordic Conference on Secure IT Systems (NordSec’23), Oslo, Norway, 16–17 November 2023. [[ePrint](#)], [[Code](#)]
- Tanveer Khan and **Antonis Michalas**. “*Learning in the Dark: Privacy-Preserving Machine Learning using Function Approximation*”. In Proceedings of the 22nd IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom’23), Exeter, U.K., November 1–3 2023. [[ePrint](#)], [[Code](#)], [CORE Ranking](#): B
- Khoa Nguyen, Tanveer Khan and **Antonis Michalas**. “*Split Without a Leak: Reducing Privacy Leakage in Split Learning*”. In Proceedings of the 19th EAI International Conference on Security and Privacy in Communication Networks (SecureComm’23), Hong Kong SAR, Hong Kong, 19–21 October 2023. [[ePrint](#)], [[Code](#)], [CORE Ranking](#): C
- Reyhaneh Rabbaninejad, Behzad Abdolmaleki, Giulio Malavolta, **Antonis Michalas** and Amir Nabizadeh. “*stoRNA: Stateless Transparent Proofs of Storage-time*”. In Proceedings of the 28th European Symposium on Research in Computer Security (ESORICS’23). Hague, the Netherlands, September 25–29, 2023. [[ePrint](#)], [CORE Ranking](#): A
- Tanveer Khan, Khoa Nguyen, **Antonis Michalas** and Alexandros Bakas. “*Love or Hate? Share or Split? Privacy-Preserving Training Using Split Learning and Homomorphic Encryption*”. In Proceedings of the 20th Annual International Conference on Privacy, Security & Trust (PST’23). Copenhagen, Denmark, August 21–23, 2023. [[ePrint](#)], [CORE Ranking](#): C
- Reyhaneh Rabbaninejad, Bin Liu, **Antonis Michalas**. “*PoRt: Non-Interactive Continuous Availability Proof of Replicated Storage*”. In Proceedings of the 38th ACM/SIGAPP Symposium On Applied Computing (SAC’23). Tallinn, Estonia, March 27–April 2, 2023. [CORE Ranking](#): B
- Reyhaneh Rabaninejad, Alexandros Bakas, Eugene Frimpong, and **Antonis Michalas**. “*A Secure Bandwidth-Efficient Treatment for Dropout-Resistant Time-Series Data Aggregation*”. In Proceedings of the first Workshop on Privacy Preserving Computation in Pervasive Computing (PrivaCom 2023) in conjunction with IEEE International Conference on Pervasive Computing and Communications (PerCom 2023), 13-17 March, 2023, Atlanta, USA.

2022.

- Bin Liu, **Antonis Michalas** and Bogdan Warinschi. “*Cryptographic Role-Based Access Control, Reconsidered*”. Proceedings of the 16th International Conference on Provable and Practical Security (ProvSec’22), Nanjing, China, 11–12 November 2022. [[ePrint](#)], [CORE Ranking](#): C
- Robert Cantaragiu, **Antonis Michalas**, Eugene Frimpong and Alexandros Bakas. “*MetaPriv: Acting in Favor of Privacy on Social Media Platforms*”. Proceedings of the 18th EAI International Conference on Security and Privacy in Communication Networks (SecureComm’22), Kansas City, United States, October 17–19, 2022. [[ePrint](#)], [[Code](#)]
- Alexandros Bakas, Eugene Frimpong and **Antonis Michalas**. “*Symmetrical Disguise: Realizing Homomorphic Encryption Services from Symmetric Primitives*”. Proceedings of the 18th EAI International Conference on Security and Privacy in Communication Networks (SecureComm’22), Kansas City, United States, October 17–19, 2022. [[ePrint](#)], [[Code](#)], [CORE Ranking](#): C
- Alexandros Bakas, **Antonis Michalas**, Eugene Frimpong and Reyhaneh Rabbaninejad. “*Feel the Quantum Functioning: Instantiating Generic Multi-Input Functional Encryption from Learning with Errors*”. Proceedings of the 36th Annual WG 11.3 Conference on Data and Applications Security and Privacy (DBSec’22), Newark, NJ, USA, July 18–20, 2022. [[ePrint](#)], [[Code](#)], [CORE Ranking](#): B
- Alexandros Bakas, **Antonis Michalas** and Tassos Dimitriou. “*Private Lives Matter: A Differential Private Functional Encryption Scheme*”. In Proceedings of the 12th ACM Conference on Data and Application Security and Privacy (CODASPY’22), April 24–26, 2022. Baltimore-Washington DC Area, United States. [[ePrint](#)]

2021.

- Ignacio M. Delgado-Lozano, Macarena C. Martínez-Rodríguez, Alexandros Bakas, Billy Brumley and **Antonis Michalas**. “*Attestation Waves: Platform Trust via Remote Power Analysis*”. In Proceedings of the 20th International Conference on Cryptology and Network Security (CANS’21), December 13-15, 2021, Vienna, Austria. [[ePrint](#)], [CORE Ranking](#): B
- Eugene Frimpong, Reyhaneh Rabbaninejad and **Antonis Michalas**. “*Arrows in a Quiver: A Secure Certificateless Group Key Distribution Protocol for Drones*”. In Proceedings of the 26th Nordic Conference on Secure IT Systems (NordSec), 29–30 November 2021, Tampere University (Virtual Event).
- Tanveer Khan, Alexandros Bakas and **Antonis Michalas**. “*Blind Faith: Privacy - Preserving Machine Learning Using Function Approximation*”. In Proceedings of the 26th IEEE International Conference on Communications (ISCC’21), Athens, Greece, September 5–8, 2021. [[ePrint](#)], [[Code](#)], [CORE Ranking](#): B // (**Best Student Paper Award**).
- Alexandros Bakas and **Antonis Michalas**. “*Nowhere to Leak: A Multi-Client Forward and Backward Private Symmetric Searchable Encryption Scheme*”. Proceedings of the 35th Annual WG 11.3 Conference on Data and Applications Security and Privacy (DBSec’21), Clagary, Canada, July 19–20, 2021. [[ePrint](#)], [[Code](#)], [CORE Ranking](#): C

2020.

- Alexandros Bakas, **Antonis Michalas** and Amjad Ullah. “(F)unctional Sifting: A Privacy-Preserving Reputation System Through Multi-Input Functional Encryption”. Proceedings of the 25th Nordic Conference on Secure IT Systems (NordSec'20), Online, November 23 – November 25, 2020. [[ePrint](#)]
- Alexandros Bakas and **Antonis Michalas**. “Multi-Input Functional Encryption: Efficient Applications from Symmetric Primitives”. In Proceedings of the 19th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, December 29, 2020 – January 1, 2021. [[ePrint](#)], CORE Ranking: A
- Tanveer Khan and **Antonis Michalas**. “Trust and Believe – Should We? Evaluating the Trustworthiness of Twitter Users”. In Proceedings of the 4th International Workshop on Cyberspace Security in Conjunction with the IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, December 29, 2020 – January 1, 2021. [[ePrint](#)]
- Hai-Van Dang, Amjad Ullah, Alexandros Bakas and **Antonis Michalas**. “Attribute-Based Symmetric Searchable Encryption”. Proceedings of the 2nd Workshop on Cloud Security and Privacy (Cloud S&P) in Conjunction with the 18th International Conference on Applied Cryptography and Network Security (ACNS'20), Rome, Italy, October 19 – 22, 2020. [[ePrint](#)]
- Alexandros Bakas and **Antonis Michalas**. “Power Range: Forward Private Multi-Client Symmetric Searchable Encryption with Range Queries”. In Proceedings of the 25th IEEE International Conference on Communications (ISCC'20), Rennes, France, 2020. [[ePrint](#)], CORE Ranking: B
- Eugene Frimpong, Alexandros Bakas, Hai-Van Dang and **Antonis Michalas**. “Do not tell me what I cannot do! (The constrained device shouted under the cover of the fog): Implementing Symmetric Searchable Encryption on Constrained Devices”. In Proceedings of the 5th International Conference on IoT, BigData and Security (IoTBDs'20). Prague, Czech Republic, May 7-9, 2020. [[ePrint](#)]
- Eugene Frimpong and **Antonis Michalas**. “IoT-CryptoDiet: Implementing a Lightweight Cryptographic Library based on ECDH and ECDSA for the Development of Secure and Privacy-Preserving Protocols in Contiki-NG”. In Proceedings of the 5th International Conference on IoT, BigData and Security (IoTBDs'20). Prague, Czech Republic, May 7-9, 2020. [[ePrint](#)] // **(Best Student Paper Award)**
- Eugene Frimpong and **Antonis Michalas**. “SeCon-NG: Implementing a Lightweight Cryptographic Library based on ECDH and ECDSA for the Development of Secure and Privacy-Preserving Protocols in Contiki-NG”. In Proceedings of the 35th ACM/SIGAPP Symposium On Applied Computing (SAC'20). Brno, Czech Republic, March 30-April 3, 2020. [[ePrint](#)], CORE Ranking: B (Accepted as a Short Paper).
- **Antonis Michalas** and Tamas Kiss. “Charlie and the CryptoFactory: Towards Secure and Trusted Manufacturing Environments”. In Proceedings of the 20th IEEE Mediterranean Electrotechnical Conference (MELECON'20). Palermo, Italy, June 16-18, 2020. [[ePrint](#)]

2019.

- **Antonis Michalas**, Alexandros Bakas, Hai-Van Dang and Alexandr Zalitko. “*MicroSCOPE: Enabling Access Control in Searchable Encryption with the use of Attribute-based Encryption and SGX*”. Proceedings of the 24th Nordic Conference on Secure IT Systems (NordSec’19), Aalborg, Denmark, November 18 – November 20, 2019. [\[ePrint\]](#)
- **Antonis Michalas**, Alexandros Bakas, Hai-Van Dang and Alexandr Zalitko. “*Access Control in Searchable Encryption with the use of Attribute-Based Encryption and SGX*”. Proceedings of the 10th ACM Cloud Computing Security Workshop (CCSW) in Conjunction with ACM Conference on Computer and Communications Security (CCS’19), London, U.K., November 11 – November 15, 2019 [\[ePrint\]](#) (Accepted as a Short Paper).
- Alexandros Bakas and **Antonis Michalas**. “*Modern Family: A Revocable Hybrid Encryption Scheme Based on Attribute-Based Encryption, Symmetric Searchable Encryption and SGX*”. In Proceedings of the 15th EAI International Conference on Security and Privacy in Communication Networks (SecureComm’19). Orlando, United States, October 23 – 25, 2019. [ePrint](#), CORE Ranking: B
- **Antonis Michalas**. “*The Lord of the Shares: Combining Attribute-Based Encryption and Searchable Encryption for Flexible Data Sharing*”. In Proceedings of the 34th ACM/SIGAPP Symposium On Applied Computing (SAC’19). Limassol, Cyprus, April 08 – 12, 2019. [ePrint](#), CORE Ranking: B
- Marcela Tuler de Oliveira, **Antonis Michalas**, Adrien E. D. Groot, Henk A. Marquering and Silvia Olabariaga. “*Red Alert: Break-Glass Protocol to Access Encrypted Medical Records in the Cloud*”. Proceedings of the 19th IEEE International Conference on E-health Networking, Application & Services (Healthcom), October 14 - 16, 2019, Bogota, Colombia. [ePrint](#), CORE Ranking: C

2018.

- Nicolae Paladi, **Antonis Michalas** and Hai-Van Dang. “*Towards Secure Cloud Orchestration for Multi-Cloud Deployments*”. In Proceedings of the 5th Workshop on CrossCloud Infrastructures & Platforms (CrossCloud’18) in Conjunction with EuroSys 2018, Porto, Portugal, April 23 – 26, 2018. [\[ePrint\]](#)

2017.

- **Antonis Michalas** and Rohan Murray. “*MemTri: A Memory Forensics Triage Tool using Bayesian Network and Volatility*”. Proceedings of the 9th ACM CCS International Workshop on Managing Insider Security Threats (MIST’17) in Conjunction with ACM CCS 2017, Dallas, USA, October 30 – November 03, 2017. [\[ePrint\]](#)
- **Antonis Michalas** and Ryan Murray. “*Keep Pies Away from Kids: A Raspberry Pi Attacking Tool*”. Proceedings of the 1st ACM CCS International Workshop on Internet of Things Security and Privacy (IoT S&P’17) in Conjunction with ACM CCS 2017, Dallas, USA, October 30 – November 03, 2017 [\[ePrint\]](#) (Accepted as a Poster/Short Paper).
- Jose Costa and **Antonis Michalas**. “*Middle Man: An Efficient Two-Factor Authentication Framework*”. Proceedings of the 3rd IEEE International Conference On Computing, Communication, Control And Automation, Pune, India, August 17-18, 2017. (Invited).
- **Antonis Michalas** and Noam Weingarten. “*HealthShare: Using Attribute-Based Encryption for Secure Data Sharing Between Multiple Clouds*”. Proceedings of the 30th IEEE International Symposium on Computer-Based Medical Systems (CBMS’17), Thessaloniki, Greece, 2017. [\[ePrint\]](#)

2016.

- **Antonis Michalas** and Kassaye Yitbarek Yigzaw. “*LocLess: Do You Really Care Your Cloud Files Are?*”. Cloud Security and Data Privacy by Design (CloudSPD’16), Workshop co-located with the 9th IEEE/ACM International Conference on Utility and Cloud Computing, Luxembourg, December 12-15, 2016. [\[ePrint\]](#)
- **Antonis Michalas**. “*Sharing in the Rain: Secure and Efficient Data Sharing for the Cloud*”. Proceedings of the 11th IEEE International Conference for Internet Technology and Secured Transactions (ICITST’16), Barcelona, Spain, December 5-7, 2016. [\[ePrint\]](#)
- **Antonis Michalas** and Thanassis Giannetsos. “*The Data of Things: Strategies, Patterns and Practice of Cloud-based Participatory Sensing*”. International Conference on Innovations in Info-business and Technology (ICIIT), Sri Lanka, March 4-5, 2016. (Position Paper)

2015.

- **Antonis Michalas** and Rafael Dowsley. “*Towards Trusted eHealth Services in the Cloud*”. Cloud Security and Data Privacy by Design (CloudSPD’15), Workshop co-located with the 8th IEEE/ACM International Conference on Utility and Cloud Computing, Limassol, Cyprus, December 7-10, 2015. [\[ePrint\]](#)
- Y. Verginadis, **Antonis Michalas**, P. Gouvas, G. Schiefer, G. Hubsch and I. Paraskakis. “*PaaS-word: A Holistic Data Privacy and Security by Design Framework for Cloud Services*”. In the 5th International Conference on Cloud Computing and Services Science (CLOSER’15), 20-22 May, 2015, Lisbon, Portugal. [\[ePrint\]](#) (Position Paper)

2014.

- **Antonis Michalas**, Nicolae Paladi and Christian Gehrman. “*Security Aspects of e-Health Systems Migration to the Cloud*”. Proceedings of the 16th IEEE International Conference on E-health Networking, Application & Services (Healthcom), October 15 - 18, 2014, Natal, Brazil. [\[ePrint\]](#) CORE Ranking: C
- Nicolae Paladi, **Antonis Michalas** and Christian Gehrman. “*Domain Based Storage Protection with Secure Access Control for the Cloud*”. The 2014 International Workshop on Security in Cloud Computing, held in conjunction with the 9th ACM Symposium on Information, Computer and Communications Security (ASIACCS), June 3, 2014, Kyoto, Japan. [\[ePrint\]](#)
- **Antonis Michalas** and Nikos Komninos. “*The Lord of the Sense: A Privacy Preserving Reputation System for Participatory Sensing Applications*”. Proceedings of the 19th IEEE International Conference on Communications (ISCC’14), Madeira, Portugal, 2014. [\[ePrint\]](#) CORE Ranking: B
- Nicolae Paladi and **Antonis Michalas**. “*One of Our Hosts in Another Country: Challenges of Data Geolocation in Cloud Storage*”. Proceedings of the 6th IEEE Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), May 11 - 14, 2014, Aalborg, Denmark. (Invited)

2012.

- **Antonis Michalas** and Menelaos Bakopoulos. “*SecGOD - Google Docs: Now I Feel Safer!*”. Proceedings of the 7th IEEE International Conference for Internet Technology and Secured Transactions (ICITST’12), London, UK, 2012. [\[ePrint\]](#)
- **Antonis Michalas**, Menelaos Bakopoulos, Nikos Komninos and Neeli R. Prasad. “*Secure & Trusted Communication in Emergency Situations*”. Proceedings of the 35th IEEE Sarnoff Symposium, Newark, New Jersey, USA, 2012. [\[ePrint\]](#)
- Tassos Dimitriou and **Antonis Michalas**. “*Multi-Party Trust Computation in Decentralized Environments*”. Proceedings of the 5th IFIP International Conference on New Technologies, Mobility & Security (NTMS’12), Istanbul, Turkey, 2012. [\[ePrint\]](#)

2011.

- **Antonis Michalas**, Tassos Dimitriou, Thanassis Gianetsos, Nikos Komninos and Neeli R. Prasad. "Vulnerabilities of Decentralized Additive Reputation Systems Regarding the Privacy of Individual Votes". Proceedings of the 3rd International ICST Conference on Security and Privacy in Mobile Information and Communication Systems (MobiSec'11), Aalborg, Denmark, 2011. [\[ePrint\]](#) // **(Best Paper Award)**
- **Antonis Michalas**, Vladimir A. Oleshchuk, Nikos Komninos and Neeli R. Prasad. "Privacy-preserving Trust Establishment scheme for Mobile Ad Hoc Networks". Proceedings of the 16th IEEE International Conference on Communications (ISCC'11), Corfu, Greece, 2011. [\[ePrint\]](#) CORE Ranking: B
- **Antonis Michalas**, Nikos Komninos and Neeli R. Prasad. "Multiplayer Game for DDoS Attacks Resilience in Ad hoc Networks". Proceedings of the 2nd IEEE International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless Vitae 2011), Chennai, India, 2011. [\[ePrint\]](#)

2010.

- **Antonis Michalas**, N. Komninos, Neeli R. Prasad and Vladimir A. Oleshchuk. "New Client Puzzle Approach for DoS Resistance in Ad hoc Networks". Proceedings of the IEEE International Conference on Information Theory and Information Security (ICITIS'10), Beijing, China, 2010. [\[ePrint\]](#)

Book 2011.

- Chapters**
- **Antonis Michalas**, Nikos Komninos and Neeli R. Prasad. "Cryptographic Puzzles and Game Theory against DoS and DDoS attacks in Networks". Encryption: Methods, Software and Security", Nova Science Publishers, 2011.

Invited Talks

- 2024/10/29 **Invited Lecture**, *BITS Pilani University, Department of Computer Science, Dubai, UAE.*
Title: From Traditional Cryptography to Advanced Cryptographic Primitives
- 2024/04/12 **Invited Lecture**, *University of Napoli Federico II, Naples, Italy, Naples, Italy.*
Title: A Short Trip into the Art of Modern Cryptography
- 2022/03/21 **Visiting Lecture**, *Secure and Networked Systems Unit., Lund University, Lund, Sweden.*
- 16/12/2019 **Keynote Speaker**, *9th International Conference on Imaging for Crime Detection and Prevention (ICDP'19), London, UK.*
Title: Fake News Outbreak 2020: Can we Stop the Virus Spreading?
- 28/11/2018 **RISE SICS and Ericsson Security Day**, *Stockholm, Sweden.*
Title: Advanced Secure Cloud Encrypted Platform for Healthcare.
- 07/09/2017 **RISE SICS Security Day**, *RISE, Stockholm, Sweden.*
Title: Trust in Public Clouds and...Keep Pies Away from Kids!
- 22/02/2017 **Panel Discussion**, *The European Information Security Summit (TEISS'17), London, UK.*
Title: Segregating third party access in the cloud.
- 17/02/2017 **Keynote Speaker**, *IEEE International Conference on Internet of Things, Next Generation Networks and Cloud Computing (ICINC'17), Pune, India.*
Title: Sharing in the Rain: Security, Privacy and Trust in Cloud Computing and Internet of Things.
- 02/03/2016 **Guest Lecture**, *IIT University, Colombo, Sri Lanka.*
Title: Introduction to Cyber Security.
- 10/03/2015 **Advances in Cryptography & Coding**, *Chalmers University, Gothenburg, Sweden.*
Title: No More Dark Clouds: Towards Trusted Cloud Environments.

- 05/02/2014 **Swedish Institute of Computer Science, Stockholm, Sweden.**
Title: Trust & Privacy in Distributed Networks.
- 04/02/2013 **Athens Information Technology, Athens, Greece.**
Title: Multi-Party Trust Computation in Decentralized Environments in the Presence of Malicious Adversaries.

In the Media

- 12/09/2017 **Short interview on CGTN Europe regarding WhatsApp's new privacy policy.**
Link: <https://tinyurl.com/7evnycre>
- 12/09/2017 **Short interview to the magazine "The Scientist" regarding the possible effects of Brexit in academia.**
Title: Scientists' Expectations for Brexit Mostly Grim
Link: <https://tinyurl.com/yc5h93c1>
- 28/06/2017 **Interview/Panel Discussion on Al Jazeera.**
Title: How can cyberattacks be stopped?
Link: <http://tinyurl.com/y7xk8p8r>
- 18/05/2017 **Article at the online magazine "Huffington Post".**
Title: Three Things We Have Learnt From The WannaCry Cyber Attack
Link: <http://tinyurl.com/yd37orqr>
- 28/03/2017 **Article at the online magazine "The Conversation".**
Title: How WhatsApp encryption works – and why there shouldn't be a backdoor
Link: <http://tinyurl.com/lt3mzsm>
- 26/03/2017 **Live Interview on Al Jazeera.**
Topic: On the 26th of March I gave a live interview at the "Newshour" show at Al Jazeera regarding the fact that UK government and secret services are asking encrypted messaging services such as WhatsApp to allow them access to users' data.
Link: <http://www.amichalas.com/blog/al-jazeera-interview-regarding-whatsapp-encryption/>
- 25/03/2017 **Interview on the Italian National Broadcasting company (RAI).**
Topic: In the wake of the March (2017) attack at Westminster, I talked about terrorism and the importance of cyber security.
Link: <http://tinyurl.com/kyeg6tp>

Awards

- 2020 **Best Student Paper Award** for the paper "*IoT-CryptoDiet: Implementing a Lightweight Cryptographic Library based on ECDH and ECDSA for the Development of Secure and Privacy-Preserving Protocols in Contiki-NG*". In Proceedings of the 5th International Conference on IoT, BigData and Security (IoTBDs'20). Prague, Czech Republic, May 7-9, 2020.
- 2017 **Staff Appreciation Award.** Students voted me as one of the best staff members in the University for the academic year 2016/17.
Where: University of Westminster, Department of Computer Science
- 2014 **ERCIM Scholarship** for conducting postdoctoral research for 1 year.
Total grant: 33,600€.

2011 **Best Paper Award** for the paper “*Vulnerabilities of Decentralized Additive Reputation Systems Regarding the Privacy of Individual Votes*”. In Mobisec, Aalborg, Denmark: 17-19 May 2011.

Academic Service

I served (or will serve) as a program committee member or editor in the following conferences and journals: PoPETS 2025, ICISSP 2025, SecureComm 2024, IEEE S&P 2023 (Oakland), PoPETS 2023, SecureComm 2023, NordSec 2023, PrivaCom@PerCom 2023, IEEE S&P 2022 (Oakland), NordSec 2022, NordSec 2021, IEEE Transactions on Dependable and Secure Computing (Associate Editor), IEEE Transactions on Cloud Computing, IEEE Transactions on Knowledge and Data Engineering, Elsevier Computers & Security Journal, Elsevier Journal of Computer and System Sciences, Springer Journal of Trust Management.

Miscellaneous

10/2023 – Current **Head of Network & Information Security Group**, TAMPERE UNIVERSITY.

I am leading the [Network & Information Security \(NISEC\)](#) research group at Tampere University.

09/2015 – 02/2018 **Head of Cyber Security Group**, UNIVERSITY OF WESTMINSTER.

I am leading the Cyber Security (CSec) research group at the University of Westminster. The primary objective of the group is to bring together expertise in education, research and practice in the field of information security and cryptography. Group members conduct research in areas spanning from the theoretical foundations of cryptography to the design and implementation of leading edge efficient and secure communication protocols. As the head of CSec, I lead research projects focused on network security and cryptography. Within a year of establishing CSec, we have successfully obtained funding for two research projects (1 EU and 1 UK) that brought to the University approximately 1,000,000€.

09/2016 – 02/2018 **Course Leader**, UNIVERSITY OF WESTMINSTER.

Since September 2016 I am the course leader for the Cyber Security and Forensics MSc offered by the University of Westminster, Department of Computer Science.

2017 **BCS Accreditation**, UNIVERSITY OF WESTMINSTER.

I have successfully participated in the BCS accreditation for the Cyber Security and Forensics MSc offered by the University of Westminster, Department of Computer Science.

</> Programming skills

Advanced PYTHON, XHTML - HTML5, CSS, JAVASCRIPT, JQUERY, PHP, .NET, C#, VB, JAVA, MYSQL, SQL SERVER, CVS/SUBVERSION

Intermediate C, ANDROID DEVELOPMENT, ORACLE, XNA FRAMEWORK

Languages

Greek **Mothertongue**

English **Cambridge FCE, TOEFL**

Spanish **Elementary**

Interests

- Traveling

- Cinema

- Literature

- Theater

- Music
- Programming
- Sports

- Photography
- Technology
- Cooking