# Kostas Papagiannopoulos

Email: kostaspap88@gmail.com, kostaspap88@protonmail.com

## 1 Personal Info

*Name & Surname:* Kostas Papagiannopoulos
*Father's & Mother's Name:* Apostolos Papagiannopoulos & Miranta Tzima
*Date & Place of Birth:* 7th of March 1988, 7/3/1988, Ioannina, Greece
*Nationality:* Greek

*Postal Address:* Plein 44, 30A, 6511 JD, Nijmegen, The Netherlands
*Visiting Address:* Digital Security Group, Institute for Computing and Information Sciences (ICIS), Mercator 1, Toernooiveld 212, 6525 EC, Nijmegen, The Netherlands

*Email Address:* kostaspap88@gmail.com, kostaspap88@protonmail.com
*Website:* kpcrypto.net
*LinkedIn:* www.linkedin.com/in/papagiannopoulos/
*Mobile Number:* +31 (0)644556416

# 2 Publications

## List


[1] C. Andrikos et al. "Location-based leakages: New directions in modeling and exploiting". In: *2017 International Conference on Embedded Computer Systems: Architectures, Modeling, and Simulation (SAMOS)*. 2017, pp. 246–252. DOI: 10.1109/SAMOS.2017.8344636.

[2] Pol Van Aubel et al. "Side-channel based intrusion detection for industrial control systems". In: *CoRR* abs/1712.05745 (2017). arXiv: 1712.05745. URL: http://arxiv.org/abs/1712.05745.

[3] Lucian Cojocar, Kostas Papagiannopoulos, and Niek Timmers. "Instruction Duplication: Leaky and Not Too Fault-Tolerant!" In: *Smart Card Research and Advanced Applications*. Ed. by Thomas Eisenbarth and Yannick Teglia. Cham: Springer International Publishing, 2018, pp. 160–179. ISBN: 978-3-319-75208-2.

[4] B. Ege et al. "Improving DPA resistance of S-boxes: How far can we go?" In: *2015 IEEE International Symposium on Circuits and Systems (ISCAS)*. 2015, pp. 2013–2016. DOI: 10.1109/ISCAS.2015.7169071.

[5] Benjamin Grégoire et al. "Vectorizing Higher-Order Masking". In: *Constructive Side-Channel Analysis and Secure Design - 9th International Workshop, COSADE 2018, Singapore, April 23-24, 2018, Proceedings*. 2018, pp. 23–43. DOI: 10.1007/978-3-319-89641-0_2. URL: https://doi.org/10.1007/978-3-319-89641-0_2.

[6] Wouter de Groot et al. "Bitsliced Masking and ARM: Friends or Foes?" In: *Lightweight Cryptography for Security and Privacy*. Ed. by Andrey Bogdanov. Cham: Springer International Publishing, 2017, pp. 91–109. ISBN: 978-3-319-55714-4.

[7] Wouter Lueks Kostas Papagiannopoulos Gergely Alpar. "Designated Attribute Proofs with the Camenisch-Lysyanskaya Signature". In: *34th WIC Symposium on Information Theory in the Benelux, Leuven, Belgium, May 30-31, 2013*.

[8] Maria Panagiotou et al. "How old is your brain? Slow-wave activity in non-rapid-eye-movement sleep as a marker of brain rejuvenation after long-term exercise in mice". In: *Frontiers in Aging Neuroscience*.

[9] Konstantinos Papagiannopoulos and Aram Verstegen. "Speed and Size-Optimized Implementations of the PRESENT Cipher for Tiny AVR Devices". In: *Radio Frequency Identification*. Ed. by Michael Hutter and Jorn-Marc Schmidt. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 161–175. ISBN: 978-3-642-41332-2.

[10] Kostas Papagiannopoulos. "Low Randomness Masking and Shuffling: An Evaluation Using Mutual Information". In: *to appear in IACR Transactions on Cryptographic Hardware and Embedded Systems, Volume 2018, Issue 3*.

[11] Kostas Papagiannopoulos and Nikita Veshchikov. "Mind the Gap: Towards Secure 1st-Order Masking in Software". In: *Constructive Side-Channel Analysis and Secure Design*. Ed. by Sylvain Guilley. Cham: Springer International Publishing, 2017, pp. 282–297. ISBN: 978-3-319-64647-3.

[12] Kostas Papapagiannopoulos. "High Throughput in Slices: The Case of PRESENT, PRINCE and KATAN64 Ciphers". In: *Radio Frequency Identification: Security and Privacy Issues*. Ed. by Nitesh Saxena and Ahmad-Reza Sadeghi. Cham: Springer International Publishing, 2014, pp. 137–155. ISBN: 978-3-319-13066-8.

[13] Stjepan Picek et al. "Confused by Confusion: Systematic Evaluation of DPA Resistance of Various S-boxes". In: *Progress in Cryptology – INDOCRYPT 2014*. Ed. by Willi Meier and Debdeep Mukhopadhyay. Cham: Springer International Publishing, 2014, pp. 374–390. ISBN: 978-3-319-13039-2.

[14] Stjepan Picek et al. "Optimality and beyond: The case of 4x4 S-boxes". In: *2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)* (2014), pp. 80–83.

## 3 Teaching Experience

- *November 2013 - May 2018* Teaching Assistant on Cryptographic Engineering course and Hardware Security course. Both courses are part of Radboud MSc on Computing Science and TRU/e MSc on Cyber Security.
- *January 2018 - March 2018* Teaching Assistant on Applied Cryptography course. The course is part of University College London (UCL) MSc on Information Security.

*Topics covered in courses:* High-performance cryptography & AVR/ARM assembly programming, side-channel analysis & countermeasures, statistical machine learning & MATLAB programming

## 4 Research Interests

- Cryptography, embedded security, cryptographic implementations
- Side-channel and fault injection attacks: correlation power analysis, template attacks, statistical distinguishers
- Side-channel and fault injection countermeasures: masking, shuffling and information-theoretic evaluations
- Laboratory evaluations with AVR, ARM Cortex-M, ARM Cortex-A, Sakura FPGA, XY table, Langer miniprobes, Langer microprobes for side-channel measurement and fault injection
- High-efficiency cryptographic implementations in software/hardware
- Lighweight cryptography
- AVR/ARM microcontrollers: high-throughput, low-latency and resource-constraint cryptographic implementations
- Intrusion/malware detection: anomaly detection against advanced persistent threats & virus polymorphism

- Information theory, statistical machine learning, neural networks
- Electronic privacy & anonymity: attribute-based credentials, zero-knowledge cryptography (Idemix, UProve), location privacy

## 5 Programming Skills

- Assembly programming (x86, AVR, ARM)
- MATLAB, OCTAVE
- NVIDIA CUDA parallel framework
- C/C++ programming, Linux and Windows OS system programming
- Web programming: Java, PHP, Google Android app development, SQL Databases & Spatial Data, HTML/CSS, Google Maps API, XMPP, SIP, Facebook API, Servlets & JSP, SOAP
- LATEX text editing

## 6 Education

**PhD in Applied Cryptography and Side-Channel Analysis** 2013–Ongoing
**Department of Digital Security, ICIS**
*Radboud University, Nijmegen, The Netherlands*

- *Winter 2018*, Research visit at Information Security group, University College London (UCL), United Kingdom
- *Winter 2015-16*, Research intership at Riscure on microprobing side-channel attacks, The Netherlands
  *Supervisors:* Lukasz Chmielewski, Ilya Kizhvatov, *Emails:* Chmielewski@riscure.com, Kizhvatov@riscure.com
- *Autumn 2014*, Study visit at Computer Security and Industrial Cryptography group (COSIC) at KU Leuven, Belgium, funded by TRUEDEVICE COST action
- Summer schools attended: Design and Security of Cryptographic Functions, Algorithms and Devices – 2013 Bulgaria, Design and security of cryptographic algorithms and devices for real-world applications – 2014 Croatia, TRUEDEVICE summer school – 2014 Portugal, IPA research school – 2015 The Netherlands

**Specialized MSc in Information Security** 2011-2013 (2 years, 120 ECTS)
**Kerckhoff's Institute for Information Security**
(currently TRU/e master in Cyber Security, `true-security.nl/`)
*Radboud University, Technical University of Eindhoven, University of Twente, The Netherlands*

- *Degree Grade:* 8.1/10 (cum laude)

- *Thesis in High-throughput lightweight ciphers for the AVR ATtiny architecture:* State of the art implementations for the PRESENT, KATAN64 and PRINCE ciphers in the AVR ATtiny context. *Thesis Grade:* 8/10.
- *Text:* `https://www.ru.nl/icis/education/master-thesis/vm/theses-archive/`
- *Supervisors:* Peter Schwabe, Lejla Batina, *Emails:* peter@cryptojedi.org, lejla@cs.ru.nl
- *Project on Malware and Antivirus.* Study on state of the art malware evasion and detection techniques. Dynamic analysis techniques, code armoring & unpacking, run-time polymorphism, GPU-assisted malware, pattern matching algorithms, *Supervisor:* Damiano Bolzoni, *Email:* damiano.bolzoni@utwente.nl
- *Link:* `https://github.com/kostaspap88/AES_CUDA_malware_unpacking/blob/master/GPUmalware%20the%20Good%20and%20the%20Bad.pdf`
- *Project: Low Latency Scalar Multiplication for VANETs.* Construction of a low-latency scalar multiplication algorithm for the P-224 curve using GPUs. Low latency and high throughput crypto primitives for ECDSA signature verification for vehicular ad hoc networks. Implementation uses mathematical and software optimizations such as GPU assembly, Karatsuba multiplication, special moduli reduction techniques for the P-224 curve and parallelized Jacobian-3 coordinates. *Supervisor:* Jonathan Petit, *Email:* j.petit@utwente.nl
- *Link:* `https://github.com/kostaspap88/p224`,
- *Project on Location Anonymity Server.* Location anonymizer based on the k-anonymity method (as described by Bugra Gedik, Ling Liu. Protecting Location Privacy with Personalized k-Anonymity).
- *Link:* `https://github.com/kostaspap88/jakas`, `http://prezi.com/ppvr-gas4rvc/location-privacy/`

**BSc, MSc in Electrical & Computer Engineering** 2005-2011 (5 years, 300 ECTS)
**School of Electrical and Computer Engineering**
*National Technical University of Athens (NTUA), Greece*

- *Degree Grade:* 8.1/10 (top 20%)
- *Thesis in Mobile Geo-Blogging:* MSc Thesis on GeoBlogging using social networks and geographical/spatial features, aiming to create a geographical social network that tracks users, landmarks and activities. Development of a mashup Android application in collaboration with Institute for the Management of Information Systems (`http://www.imsi.athenarc.gr/`), using Facebook Graph, REST, FQL, XMPP and Google Maps. *Thesis Grade:* 10/10.
- *Text (in Greek):* `http://www.dbnet.ece.ntua.gr/pubs/uploads/DIPL-2011-6.pdf`
- *App Link:* `https://www.facebook.com/geocrowdmobile`
- *Supervisor:* Timos Sellis, NTUA, IMIS, *Email:* timos@imis.athena-innovation.gr

- *Summer schools attended:* Athens Information Technology (AIT) summer school on Pervasive Networks and the Web of Things

**Highschool diploma, 3rd Public Highschool of Ioannina** 2002-2005 (3 years)
*Ioannina, Greece*

- *Grade:* 19.467 / 20.000 (top of class)

## 7 Language Skills

English Language: Professional level.

- *TOEFL iBT:* grade 116/120 (2010)
- *Cambridge University CPE:* grade C (2002)

Italian Language: Intermediate level.

- *Università di Perugia Celi 3:* grade B (2001)

Greek Language: Mother Language.

## 8 Honors & Awards

Arnaoutis Foundation: Full scholarship for post-graduate studies in Computer Science, 2012-2013

Filitou Foundation: Scholarship for undergraduate studies, 2006-2011

Cosmote Telecom: Award for undergraduate studies, 2005

Eurobank: Award for highschool top of class, 2005

United Nations Essay Writing Contest: Award in essay writing in nation-wide (Greece) competition for "Refugees World Day", 1999

## 9 Hobbies and other Activities

History books & documentaries, political analysis & commentary studying, Rowing, traditional music instrument "bouzouki", music theory & harmony,