Marios Omar Choudary

Address — University Politehnica of Bucharest, Faculty of Computer Science, Splaiul Independentei 313, Sector 6, Bucharest, Romania

E-mail — marios.choudary@upb.ro

Education

- 2018 - 2021 — **University of Bucharest**, Master in Theology, Faculty of Orthodox Theology, Bucharest, Romania

  Studies finalised with the work "Mărturii ale picturii paleologe în Ţara Românească – Mănăstirea Chora- Kahrie Djami şi Biserica Sfântul Nicolae domnesc din Curtea de Argeș" ("Whitnesses of the paleologean paintings in the Romanian Kingdom – The monastery Chora (Kharie Djami) and the Princely Church of Saint Nicholas in Curtea de Argeș").

- 2014 - 2018 — **University of Bucharest**, B.Th in Theology, Faculty of Orthodox Theology, Bucharest, Romania

  Studies finalised with the literary work "Erminia duhovnicească a Sfântului Ioan Gură de Aur la epistola Sfântului Pavel către Filipeni" ("The spiritual interpretation of Saint John Chrysostom to the epistle of Saint Paul to the Philippians").

- October 2010 - 2014 — **University of Cambridge**, PhD in Computer Science, supervised by Markus Kuhn, Cambridge, UK

  My main work has been the evaluation and improvement of template attacks, which are considered the most powerful techniques to eavesdrop on microcontrollers in order to infer data processed by the microcontroller. My research involved the development of custom printed circuit boards to allow a good evaluation of side-channel attacks, the acquisition and processing of millions of side-channel traces obtained using a digital oscilloscope, the application and development of many statistical techniques and the evaluation of many of these techniques on many datasets to evaluate the efficiency of template attacks using different acquisition parameters and post-processing algorithms. Other work during my PhD includes the development of a protocol to protect against relay attacks, protocols for peer-to-peer payments using mobile phones and smartcards and the analysis and implementation of open source code for the FileVault 2 full disk encryption.

- October 2009 - June 2010 — **University of Cambridge**, MPhil in Advanced Computer Science, Cambridge, UK

  In the first half of my MPhil I developed a fast hardware router which could perform Network Address Transaltion (NAT) at line speed (1Gbps), using the NetFPGA platform. In the second half I built a hand-held EMV (protocol used in bank smartcards) interceptor device that can intercept a transaction between a smartcard and a terminal (smartcard reader). The main goal of the project was to implement a protection against the relay

attack by showing details about the transaction (e.g. amount) so that a malicious terminal could not send to the smartcard information that is different from what is displayed on its screen. After finalising the hardware device and writing a comprehensive software stack for the smartcard ISO-7816 protocol and the EMV protocol, we used the device to reveal an important flaw in the implementation of the EMV protocol.

- October 2003 - June 2008 — **University Politehnica of Bucharest**, Computer Science Department, Bucharest, Romania

  In the last term I worked at the Institute de Recherche pour l'Informatique de Toulouse (France), doing computer vision research on mobile devices. As a result of my work I developed a mobile guide aplication that could use 3D scenes of a football stadium and location information to guide people to their seats.

Research Interests: My current research interests are on side-channel analysis, with a focus on the optimisation of security evaluations and modelling of the physical side channel leakage of various devices, particularly Systems on Chip (SoC).
I am also interested in security protocols. I did some work on exploring the security of the payment protocol EMV. More recently I have been involved in the designe of a new authenticated key exchange without the use of a trusted third party or pre-established keys, by means of using multiple public channels. We are now woring on end-to-end encryption versions of the protocol.

Selected publications

- Costin Ghiban and Marios O. Choudary, *Improved Correlation Power Analysis Attack on the Latest Cortex M4 Kyber Implementation*, Cryptography 9 (1), 19, 2025.
- A. Rădulescu, P. G. Pantelimon and Marios O. Choudary, *GE vs GM: Efficient side-channel security evaluations on full cryptographic keys*, International Conference on Cryptographic Hardware and Embedded Systems (CHES) 2022.
- P. G. Pantelimon and Marios O. Choudary, *Refinement of Massey Inequality*, IEEE International Symposium on Information Theory (ISIT) 2019, pp. 495–496.
- Sergiu Costea and Marios O. Choudary and Doru Gucea and Björn Tackmann and Costin Raiciu, *Secure Opportunistic Multipath Key Exchange*, ACM Conference on Computer and Communication Security (CCS) 2018, Toronto, Canada.
- Marios O. Choudary, Markus G. Kuhn, *Efficient, Portable Template Attacks*, IEEE Transactions on Information Forensics and Security, vol. 13 (2), pp. 490–501, 2018.
- Marios O. Choudary and P. G. Pantelimon, *Back to Massey: Impressively fast, scalable and tight security evaluation tools*, International Conference on Cryptographic Hardware and Embedded Systems (CHES) 2017, Springer LNCS 10529, pp. 367–386.
- Marios O. Choudary, Markus G. Kuhn, *Efficient stochastic methods: profiled attacks beyond 8 bits*, CARDIS 2014. LNCS 8968, pp. 85–103.
- O. Choudary, M. G. Kuhn, *Efficient Template Attacks*, CARDIS 2013, Berlin, 27–29 November 2013. LNCS 8419, pp. 253–270.

- Mike Bond, Omar Choudary, Steven J. Murdoch, Sergei Skorobogatov and Ross Anderson, *Chip and Skim: cloning EMV cards with the pre-play attack*, IEEE Symposium on Security and Privacy, 18–21 May 2014, San Jose, CA.
- O. Choudary, *The Smart Card Detective: a hand-held EMV interceptor*, MPhil thesis at University of Cambridge, 2010. Computer Laboratory Technical Report UCAM-CL-TR-827.

Major Research Projects

- **Evaluation of Side-Channel Leakage in System on Chip Devices (2018-):** This is an ongoing project, funded by a research grant from the University Politehnica of Bucharest and then continued by a research grant from UEFISCDI, in which we explore the leakage models suitable for describing and analysing side-channel leakage in System on Chip devices. Our current work is on several SoC devices, an ARM Cortex A device and a Cortex-M device, focusing on a detailed understanding of the leakage of different components as well as the development of efficient security evaluations for these devices.
- **Secure Key Exchange from Multipath Communications (2014-):** Funded by the Horizon2020 EU project SSICLOPS, in this work within our team at University Politehnica of Bucharest we have designed a secure key exchange protocol that provides security against many active MITM attackers without the need for trusted third parties such as Certificate Authorities or pre-established secret keys. This protocol, which we named SMKEX increases the security of opportunistic encryption but can also increase the security of standard TLS.

  With another recent grant from UEFISCDI we have continued the development of this protocol, by adapting it in the end-to-end encryption context.
- **Evaluation and Improvement of Template Attacks (2010-2014):** This was the main work of my PhD, under the supervision of Dr. Markus Kuhn in the Computer Laboratory, University of Cambridge. The main focus has been the optimisation of Template Attacks in various scenarios, including the security analysis sub-cryptographic routines such as copying secret keys from memory to registers. In particular, I have investigated the applicability of Template Attacks when dealing with different devices as well as their applicability when using secrets of size larger than the usual 8-bit values found in typical attacks against block ciphers. I published several papers about this work at specialized international conferences and journals.
- **Analysis of FileVault 2 full Disk Encryption:** Work done in collaboration with Joachim Metz and Felix Grobert at Google Zurich in 2011. We reverse engineered the functionality of FileVault 2 full disk encryption and produced open source code to read encrypted volumes, which is very useful to digital forensic practitioners. The associated paper is *Security Analysis and Decryption of Filevault 2*, in Advances in Digital Forensics IX, IFIP Advances in Information and Communication Technology 410, 2013, pp 349–363.
- **EMV Security Analysis:** In 2012, together with Mike Bond, Ross Anderson, Steven Murdoch and Sergei Skorobogatov, we started to analyse the security of random numbers as they are used for ATM/POS transactions with EMV and we discovered from acqusition of real traces that the unpredictable numbers used in a transaction are not as unpredictable as they should be, which can lead to what we termed a *pre-play* attack. This work is published

on arxiv.org as *Chip and Skim: cloning EMV cards with the pre-play attack*, and has been submitted to IEEE Symposium on Security and Privacy 2014.

Previously I developed the *Smart Card Detective* during my MPhil at the Computer Laboratory, which we used to analyse and show a great vulnerability of the EMV system. The details are published in *The Smart Card Detective: a hand-held EMV interceptor*, Computer Laboratory Technical Report UCAM-CL-TR-827.

We also used the Smart Card Detective to test several ideas of peer-to-peer payments. The details are in *Might Financial Cryptography Kill Financial Innovation? – The Curious Case of EMV*, Financial Cryptography and Data Security 2011, LNCS 7035.

- **Mobile Computer Vision:** In 2008-2009 I worked with Romulus Grigoras and Vincent Charvillat at IRIT (Toulouse, France), to develop new methods to visualise content and location on mobile devices. One of the most popular projects is the mobile augmented reality application for cultural heritage, where we used the Nokia CV C++ library on a Nokia N95 to project prehistoric animal images on top of a live video stream of a cave. This work is published as *MARCH: Mobile Augmenting Reality for Cultural Heritage*, 17th ACM international conference on Multimedia, 2009.

Grants, Awards and Scholarships

- *UEFISCDI Young Teams (TE) Grant (2021-2022):* RON 432.000 (EUR 80.000) awarded in January 2021 by the UEFISCDI national research funding organisation for continuing my research on on side-channel evaluations of System on Chip devices.
- *UEFISCDI Experimental-Demonstrator Project (PED) Grant (2020-2022):* RON 600.000 (EUR 120.000) awarded in August 2020 by the UEFISCDI national research funding organisation for the implementation of the client-to-client version of our SMKEX protocol, in collaboration with CERTSIGN.
- *UPB CRC scholarship:* EUR 36000 Awarded in June 2018 by the University Politehnica of Bucharest for the continuation of my research on side-channel evaluations of System on Chip devices.
- *UPB GEX scholarship:* EUR 18000 Awarded in September 2016 by the University Politehnica of Bucharest for the continuation of my research on side-channel evaluations of electronic devices.
- *Lundgren scholarship:* £1500 Awarded in November 2013 by the University of Cambridge for the continuation of my stipend in order to complete my PhD studies, on the basis of *great piece of work*.
- *Google Europe Doctoral Fellowship in Mobile Security:* Scholarship awarded in 2010 for a duration of 3 years (£75000 in total) to pursue my PhD studies.
- *EPSRC Studentship:* Scholarship awarded in October 2009 for one year to cover the tuition fees (around £6000) of my MPhil at the Computer Laboratory.
- *C T Taylor fund scholarship award:* Scholarship award of £3000, given in October 2009, for my MPhil at the Computer Laboratory.

- *1st prize at Windows Embedded Student Challenge 2006:* Winner of the Windows Embedded Student Challenge 2006 (now part of Imagine Cup), organised by Microsoft. Final prize of $8000.

Teaching experience:

- Since 2018, I became a senior lecturer at the University Politehnica of Bucharest, Faculty of Computer Science. I current teach Introduction to Cryptology, Signal Processing and Applied Cryptography.
- Since 2014, I became a lecturer at the University Politehnica of Bucharest, Faculty of Computer Science, teaching courses on Cryptography and Signal Processing.
- During 2010-2014, at the Computer Laboratory in Cambridge, I have been teaching small groups during supervisions in the areas of security protocols, cryptography and digital signal processing.
- In 2009, at IRIT (Toulouse, France), I have taught seminars with groups of 15-20 students on computer vision.
- In 2008 I hold seminars in computer networks at the University Politehnica in Bucharest.

Technical Skills

- **Statistical skills:** Statistical analysis, data visualisation, data compression/projection in subspaces.
- **Programming languages:** Matlab, C, C++, Python, Verilog.
- **Hardware skills:** FPGA programming (NetFPGA, Xilinx, Proxmark III), PCB design.
- **Reverse engineering skills:** Reversed engineered FileVault 2 in Mac OS X 10.7.

Languages

- Romanian, Spanish - native,
- English - fluent written and spoken,
- French - intermediate.

Other training:

During 2011-2013 I followed several online courses offered by Coursera and I completed the following (with certificates): *Machine Learning*, *Cryptography I*, *Fundamentals of Electrical Engineering*.
In 2012 I attended the summer schools: *ECRYPT II* (hardware security) in Bochum, Germany and *Cryptabit* (cryptography) in Bohn, Germany.
During 2010-2012 I followed the courses offered at the Computer Laboratory on: *Research Skills*, *Security I (cryptography)*, *Security II (security protocols)* and *Digital Signal Processing*.
In 2007-2008 I obtained Cisco CCNA and CCNP certifications.

Publications

See my Google profile for a complete list of my publications:
`https://scholar.google.com/citations?user=482_pCMAAAAJ&hl=en&oi=ao`.

Conferences and Invited Talks

- **GE vs GM: Efficient side-channel security evaluations on full cryptographic keys**, Presentation of our research paper with the same title at the International Conference on Cryptographic Hardware and Embedded Systems (CHES) 2022, Leuven, Belgium.
- **Secure Opportunistic Multipath Key Exchange**, Presentation of our research paper with the same title at the ACM Conference on Computer and Communication Security (CCS) 2018, in Toronto, Canada.
- **Back to Massey: Impressively fast, scalable and tight security evaluation tools** Presentation of our research paper with the same title at the International Conference on Cryptographic Hardware and Embedded Systems (CHES) 2017, in Taipei, Taiwan.
- **Security from Disjoint Paths: Is It Possible?** Presentation of our position paper with the same title at the Security Protocols Workshop 2017, in Cambridge, UK.
- **Efficient stochastic methods: profiled attacks beyond 8 bits** Presentation of our paper with the same title at CARDIS 2014, in Paris, France.
- **Template Attacks on Different Devices** Presentation of our paper with the same title at COSADE 2014, in Paris, France.
- **Chip and Skim: cloning EMV cards with the pre-play attack** Presentation of our paper with the same title at IEEE Symposium on Security and Privacy, San Jose, CA, 2014.
- **Efficient Template Attacks:** Presentation of our paper with the same title at the 12th Smart Card Research and Advanced Application Conference (CARDIS) 2013, in Berlin, Germany.
- **Security Analysis and Decryption of FileVault 2:** Presentation of our paper with the same title at the IFIP International Conference in Digital Forensics, Florida, US, 2013.
- **Chip and PIN internals:** Invited talk on Chip and PIN at the following locations:
  - ISSA conference, Ireland, 2011.

  - Athcon, Greece, 2011.
  - IBM Warwick, UK, 2011.
  - Munster Institute for Computer Science, Germany, 2011.

- **Chip and PIN: exploring the EMV system:** Talk preented at Darwin College, Cambridge, 2011.
- **Make noise and whisper: a solution to relay attacks:** Presentation of our paper with the same title at the Security Protocols Workshop, Cambridge, 2011.
- **Might Financial Cryptography Kill Financial Innovation? The Curious Case of EMV:** Presentation of our paper with the same title at the Financial Cryptography 2011 conference, St. Lucia.

References

- **Costin Raiciu:** Senior Lecturer at the Faculty of Computer Science, University Politehnica of Bucharest, RO.
  Website: `http://nets.cs.pub.ro/~costin/`
- **Markus Kuhn:** Senior Lecturer at the Computer Laboratory, University of Cambridge, UK.
  Website: `http://www.cl.cam.ac.uk/~mgk25/`
- **Virgil Gligor** Professor at Carnegie Mellon University, US.
  Website: `https://www.ece.cmu.edu/directory/bios/gligor-virgil.html`

Conf. Dr. Marios O. Choudary,