Estuardo Alpírez Bock

Since July 2020 I've been a Postdoc at Aalto University, working at the Cryptography group with Prof. Chris Brzuska. Before that, I completed my PhD under his supervision, co-advised by Wil Michiels from NXP Eindhoven. My research focuses on White-Box Cryptography. Further research interests include side channel analysis attacks and the design and implementation of cryptographic algorithms in hardware.

Employment History

Postdoc Researcher
Aalto University
July 2020 - *present*
Helsinki, Finland
Postdoctoral Researcher at the department of Mathematics and Systems Analysis at Aalto University in Finland, working in the group of Chris Brzuska. Research topics include attacks on White-Box Cryptography as well as the study of feasibility results for White-Box Cryptography. Additionally working as a teaching assistant of the course on Cryptography and Data Security.

Internship
Visa Research
February 2020 – May 2020
Palo Alto, California
Internship at Visa Research under the supervision of Gaven Watson and in collaboration with Shashank Agrawal and Yilei Chen, where we embraced research related to the secure design and distribution of mobile payment applications

PhD-Student
Aalto University
April 2018 – June 2020
Helsinki, Finland
PhD student of Prof. Chris Brzuska at the department of Mathematics and Systems Analysis at the Aalto University in Finland. Research topics include attacks on White-Box Cryptography as well as the study of feasibility results for White-Box Cryptography. Additionally working as a teaching assistant of the course on Cryptography and Data Security from Prof. Brzuska.
Work in cooperation with Wil Michiels (NXP Eindhoven) and Joppe Bos (NXP Leuven) on automated attacks on white-box cryptography as well as on defining and studying security notions and feasibility results for white-box cryptography

Guest Scientist
Eindhoven University of Technology
January 2017 – March 2017
Eindhoven, Netherlands
Guest scientist of Prof. Wil Michiels and Alessandro Amadori at the department of Mathematics and Computer Science and Embedded Networked Systems at Eindhoven University of Technology. During this period, we studied the possibility of extending and improving automated attacks on white-box cryptographic implementations.

PhD-Student
Hamburg University of Technology
November 2016 – March 2018
Hamburg, Germany
PhD student of Prof. Chris Brzuska at the Institute for IT-Security Analysis. Research topics include attacks on White-Box Cryptography as well as Security Notions for White-Box Cryptography. Additionally worked as a teaching assistant of the course on Introduction to IT-Security from Prof. Brzuska and Prof. Gollmann.
Work in cooperation with Wil Michiels (NXP Eindhoven) and Joppe Bos (NXP Leuven) on automated attacks on white-box cryptography as well as on defining security notions for white-box cryptography

Scientist/PhD-Student
IHP GmbH
November 2015 – October 2016
Frankfurt (Oder), Germany
Scientist on the System Design department. Research topics include elliptic curve cryptography and side channel analysis attacks.
Skills gained/used: team work, work in projects, implementation of cryptographic hardware accelerators, vulnerability assessment of cryptographic implementations, implementation of drivers for wireless sensor nodes, programming in VHDL, programming in C, writing of scientific papers

Student Assistant
Technical University of Cottbus-Senftenberg
November 2014 – October 2015
Cottbus, Germany
Student assistant at the chair "Sicherheit in pervasiven Systemen (Pervasive System Security)"
Skills gained/used: working in teams, planning for projects, programming in VHDL, application of statistical methods for the analysis of cryptographic implementations, programming in Python, writing of scientific papers

Student Assistant
IHP GmbH
June 2014 – October 2014
Frankfurt (Oder), Germany
Student assistant on the theme "Implementing Elliptic Curve Cryptography under Consideration of Side Channel Analysis Attacks"
Skills gained/used: programming in VHDL, application of statistical methods for the analysis of cryptographic implementations, programming in Python, writing of scientific papers, time management skills

Education History

Technical University of Cottbus-Senftenberg, Germany
April 2013 – October 2015
Master of Science in Information and Media Technology. Specialization area: Communication and Media Technologies

Master thesis in collaboration with IHP – Innovations for High Performance Microelectronics on the subject "SCA Resistant Implementation of the Montgomery *kP*-Algorithm" – passed with the grade 1,0 (very good) and distinguished with the faculty award for an excellent master thesis in the curse of studies of Information and Media Technology

Technical University of Cottbus, Germany
October 2008 – April 2013
Bachelor of Science in Information and Media Technology

Bachelor thesis in collaboration with the chair Communication Technology on the subject "Visualization of the Convolution Operation"

University of Milan, Italy
September 2009- August 2010 (2 semesters)
University exchange through the ERASMUS program
Courses taken (all in Italian language): Analysis, Operating Systems, Audio-Informatics, Electronics, Electronics (Lab), Digital Electronics, Digital Electronics (Lab), Statistics, Graphic-Informatics

University for Foreigners of Siena, Italy
August 2009
EILC Intensive Italian language course (B1) for ERASMUS exchange students

Studienkolleg for foreign students at the University of Hamburg, Germany
August 2007 – July 2008
Feststellungsprüfung Medicine-Course

German language courses in Hamburg, Germany
Attended institutes: Inlingua, World University Service (WUS)
October 2006 – May 2007

High School: Colegio Internacional Montessori in Guatemala City, Guatemala
January 2002 – October 2006
High School Diploma (English-Spanish)

Languages

Spanish Mother tongue

English Fluent – native level (written, reading, spoken)

German Fluent – native level (written, reading, spoken)

Italian Fluent (written, reading, spoken)

Finnish Intermediate (B1 level on writing, reading and speaking)

Publications

On the Foundations of White-Box Cryptography.
PhD Thesis, https://aaltodoc.aalto.fi/handle/123456789/44380

Security Reductions for White-Box Key-Storage in Mobile Payments.
E. Alpirez Bock, C. Brzuska, M. Fischlin, C. Janson, W. Michiels.
In ASIACRYPT 2020: https://eprint.iacr.org/2019/1014

Security Assessment of White-Box Design Submissions of the CHES 2017 CTF Challenge.
E. Alpirez Bock, C. Brzuska, M. Fischlin, C. Janson, W. Michiels.
In COSADE 2020: https://eprint.iacr.org/2020/342

On the Security Goals of White-Box Cryptography.
E. Alpirez Bock, A. Amadori, C. Brzuska, W. Michiels.
In TCHES 2020: https://eprint.iacr.org/2020/104

White-Box Cryptography: Don't Forget About Grey Box Attacks.
E. Alpirez Bock, J. W. Bos, C. Brzuska, C. Hubain, W. Michiels, C. Mune, E. Sanfelix Gonzalez, P. Teuwen, A. Treff. In Journal of Cryptology (2019): https://eprint.iacr.org/2017/355

Doubly Half-Injective PRGs for Incompressible White-box Cryptography.
E. Alpirez Bock, A. Amadori, J. W. Bos, C. Brzuska, W. Michiels.
In CT-RSA 2019: https://eprint.iacr.org/2019/329

On the Ineffectiveness of Internal Encodings - Revisiting the DCA Attack on White-Box Cryptography.
E. Alpirez Bock, C. Brzuska, W. Michiels, A. Treff. In ACNS 2018: https://eprint.iacr.org/2018/301

Inherent Resistance of Efficient ECC Designs against SCA Attacks.
Z. Dyka, E. Alpirez Bock, I. Kabin, P. Langendörfer.
In Proceedings of the 8th IFIP International Conference on New Technologies, Mobility and Security, IEEE, 2016: https://ieeexplore.ieee.org/document/7792457

Increasing the Robustness of the Montgomery kP-Algorithm against SCA by Modifying its Initialization.
E. Alpirez Bock, Z. Dyka, P. Langendörfer.
In Proceedings of the 9th International Conference for Information Technology and Communication, Springer, 2016: https://link.springer.com/chapter/10.1007/978-3-319-47238-6_12

SCA Resistant Implementation of the Montgomery kP-Algorithm.
Master thesis, https://opus4.kobv.de/opus4-btu/frontdoor/index/index/docId/3628, 2015