Editorial

UbiCrypt successfully completed its 3rd year and the Research Training Group is constantly growing into shape. The group currently holds 13 Principal Investigators, 2 Postdoctoral Researchers, 20 PhD Students, 2 Qualifying Fellows and 9 Student Assistants. This broad range covers all stages of an academic career and therefore best prepares the UbiCrypt offspring for upcoming steps. This variety opens the opportunity to work within as well as across the own peer-group.

We welcome Prof. Markus Dürmuth and Prof. Sebastian Faust in our group, who will support and supervise our students as new Principal Investigators. We’re especially delighted to announce that UbiCrypt holds its first five alumni, who successfully graduated from the program and now pursue their careers in well renowned institutions such as Microsoft Research, Cambridge or Infineon, Munich.

In the last academic year we look back on lots of successful interesting and fun events: our students represented UbiCrypt and the framing Horst Görtz Institute for IT-Security (HGI) at BlauPause, the university’s street festival to celebrate its 50th anniversary. Our annual summer school focussed on SYSTEMS SECURITY from a broad perspective - an excellent opportunity for exchange with top international researchers. The achievements of the year were summarized at the annual Research Retreat, which took part at Westerholt Castle. For the first time, the individual presentations in front of the whole UbiCrypt group were followed by an additional PhD day to give room for feedback on the program and further social events.

We’re proudly looking back at an eventful academic year and we hope you enjoy the read!

Prof. Dr. Alexander May
Speaker DFG-Research Training Group UbiCrypt
The Research Training Group UbiCrypt gathers excellent scholars from all IT-Security related disciplines as well as from almost every level of an academic career. The members of UbiCrypt stem from every stage of the scientific career: Bachelor students, Master students in our fast-track PhD program, doctoral students, post-docs and, of course, junior and established professors.

The core focus of UbiCrypt is the training program for doctoral students. They are supervised by the Principal Investigators (PIs) and mentored by the Interdisciplinary Coordinators. The duality of disciplinary supervision and working spaces in their departments on the one hand and the structured interdisciplinary exchange at UbiCrypt on the other hand best prepares the students for a broad range of academic positions.

With one-year-lasting scholarships the Qualification Fellows join the group after having successfully completed their Bachelor program with exceptional grades. In cooperation with TopING, an initiative by the Faculty for Electrical Engineering and Information Technology of Ruhr-Universität Bochum, a fast track option can be offered to talented young researchers.

To make sure that prospective scholars get the chance to gain practical experience as early as possible, UbiCrypt provides positions as research students at the chairs and working groups involved in the Research Training Group. These positions are meant to give precious insights in the possibly upcoming life as ITS scholar.

On the following pages, we will further elaborate on the several components of UbiCrypt.
Training Program

The over-all objective of the Research Training Group is to provide a doctoral education in modern IT-security at a top international level. In order to combine cutting-edge research, interdisciplinarity, preparation for industrial and academic careers with a dissertation period of three years, a structured training plan is the key feature of UbiCrypt, in addition to classical doctoral research.

Therefore, the training program of UbiCrypt ranges from general to specialized educational parts. To complement the individual dissertation research a variety of disciplinary and crossdisciplinary offers are created to support the academic career development of the UbiCrypt PhD Students. UbiCrypt closely collaborates with the RUB Research School to provide a broad inter- and transdisciplinary offer for young researchers.
PhD Lecture

Each PhD student attends two courses on IT-Security. Typically, the courses should be taken in the first year of her/his doctorate studies. We offer novel courses on the PhD level which are specifically dedicated to the research topics of the UbiCrypt group. The courses may include complementary components, such as work with relevant literature or a project part. Every semester at least one new course will be offered.

In the last academic year the lectures were given by Prof. Sebastian Faust, Prof. Christina Pöpper and Prof. Gregor Leander:

Winter term 2014/15:
Financial Cryptography - Prof. Sebastian Faust

Summer term 2015:
Private and Anonymous Communication - Prof. Christina Pöpper
Symmetrische Kryptanalyse - Prof. Gregor Leander

These PhD Lectures are also open to RUB PhD students and other interested scholars. UbiCrypt is pleased to present current research outcome of its Principal Investigators to a broad academic public.
Seminar & Lecture Series

We offer a research-oriented series of lectures for all PhD Students of the Research Training Group. It takes place every two weeks and is intended for PhD Students with and without stipend support. Primarily, external speakers from academia and industry will present new scientific results, or will give an overview of a specific research area. The lecture series takes place during the semester only. The goal of the lecture series is to offer a broad scientific education in modern IT-security, as well as an opportunity for students to get in touch with external (international) researchers.

In addition to the lecture series, we will also offer a biweekly PhD Student Seminar; thus, there will be a lecture or seminar every week on a regular basis. In the PhD Student Seminar the members of UbiCrypt will give talks on their current research results. Each PhD Student is supposed to give a presentation once per year. The goal of the seminar is to encourage scientific discussions, and to keep all member of UbiCrypt informed about each other’s ongoing research. Attendance of both the seminar and the lecture series is mandatory for the PhD Students. A 70% attendance rate must be achieved by each student.
Crossdisciplinary Project

Every PhD student is supervised by at least two PIs from the UbiCrypt group. In order to assure that every student benefits from the dual advisor concept, each PhD student performs a six-week “cross-disciplinary” project in the second advisor’s group. To further strengthen this educational aspect over the duration of the dissertation, post-docs will act as interdisciplinary coordinators. In most cases, this project will directly contribute to the dissertation research.

The work conducted in this phase should have project character and the student’s workplace will be at the host group during this time. In most cases, the visiting student will work with a post-doc or an advanced Ph.D. student of the host group. We hope that this has a positive long-term effect on the cohesiveness of UbiCrypt. Moreover, gaining insight into the working techniques used in related disciplines, with possibly different research cultures, enables a student to collect valuable experiences for her/his later career.

Research Visit

Our PhD students are warmly encouraged to pursue one or more research visits at well-renowned institutions abroad. The six to eight weeks stints at leading international institutions help to establish our young scholars in the academic as well as the industrial community. They develop own projects such as joint publications with new scholars or undertake internships to bridge the gap between scholarship and practical application.

For instance, previous research visits have taken our PhD students taken to the University of Massachusetts in Amherst/USA, Microsoft Research in Cambridge, and NTT Japan in Tokyo.
Events

In 2014/2015 we had the chance to not only pursue our traditional annual events, but to also support additional conferences in order to broaden the overall UbiCrypt program. These collaborations with other formats enrich the UbiCrypt network and provide various platforms for sharing academic ideas with other interested scholars.

In May, the traditional workshop HackPra Allstars was held framed by the OWASP conference in Amsterdam, which brought together a compilation of HackPra’s most fascinating talks from the past academic year.

Our university celebrated its 50th anniversary in June with a festive week filled with multifaceted events. The closing street festival BlauPause included a counter by our UbiCrypt students. With the campaign “Solve a riddle - get a cookie!” the principals of cryptographic research were playfully presented to a broader public.

The annual Summer School SYSTEMS SECURITY took place in July and was hosted by Prof. Thorsten Holz, who created an intimate event with lectures and sessions on all facets of according research.

Our Research Retreat traditionally gathered the entire UbiCrypt group at a three-day-event at Westerholt Castle. The PhD and postdoctoral researchers presented their ongoing projects and took benefit from the PI’s interdisciplinary support.

LightSec 2015 invited international scholars with focus on Lightweight Security to gather in Bochum in September. The workshop was hosted by our PI Prof. Tim Güneysu.
We invite interested Postdocs, PhD and Master students to participate in our

SUMMER SCHOOL

SYSTEMS SECURITY

DFG-Research Training Group UbiCrypt
Ruhr-University Bochum
July 20-23, 2015

For further information and registration please visit our webpage:
ubicrypt.hgi.rub.de
facebook.com/ubicrypt
Summer School
SYSTEMS SECURITY
(July 20-23, 2015)

From July 20-23, 2015 UbiCrypt invited to its third Summer School, which traditionally took place at Ruhr-University Bochum. This year the event was organized by the Chair for Systems Security (http://syssec.rub.de) and put special focus on research topics related to software security, in particular code-reuse attacks.

The UbiCrypt Summer School SYSTEMS SECURITY gave the opportunity to Master and PhD students as well as young scholars to learn more about software security. It was designed as a mix of lectures and hands-on exercises, allowing the students to learn how to find and abuse vulnerabilities in (binary) software as well as to review potential defenses. Furthermore, we offered a multifaceted program with exercises on the topics covered in the lectures.

Topics covered during the summer school include (e.g.):

• Finding vulnerabilities in source code or binaries
• Developing exploits
• Binary analysis techniques such as symbolic execution or taint analysis
• Code-reuse attacks such as return-oriented programming
• Software defenses against code-reuse attacks

The sessions of the Summer School were complemented by a workshop by Prof. Thorsten Holz, who presented methods and best-practice advice concerning the academic life. The according social events lead the group to the Jahrhunderthalle with concluding drinks in Bochum’s famous Bermuda3eck.
UbiCrypt
Cryptography in Ubiquitous Computing

The PhD students of the DFG-Research Training Group UbiCrypt present their projects and share ideas at the Research Retreat.

October 5 - 7, 2015 | Westerholt Castle
Research Retreat
(October 5-7, 2015)

The traditional Research Retreat is set up as a plenary meeting of the Research Training Group. The attendance of the entire group provides an ideal framework for the discussion of questions of all substantial, strategic or organizational kind. This annual convention guarantees the involvement of every member of UbiCrypt into the main processes of the program.

The presence of scholars of all stages of the PhD period allows the exchange of experiences between doctoral students of all levels of a PhD phase. The informal atmosphere of the Research Retreat gives room for feedback not only on the individual progress, but also on presentation skills and techniques.

Concepted as a three-day-event at a location outside the Ruhr-Universität the Research Retreat aims to put exclusive focus on the recent developments of the individual dissertations. All scholarship holders and associated collegiates present the status of their projects in a series of talks. The group of Principal Investigators joins the audience and gives time for questions, answers and interdisciplinary advice. The annual gathering is part of UbiCrypt’s quality management as the PI’s individual feedback for their doctoral students is supplemented by a broader group from various disciplines. With this, constructive feedback from fellow collegues and specialists from related disciplines as well as various exterior views can be guaranteed.

This year, the event took place at WesterholtCastle in the Münsterland, a traditional location apart from the lively Ruhr-Universität. The excursion left room for social networking while exploring new sports: some UbiCrypters played golf for the first time. The additional PhD day, a new aspect of the Research Retreat, gave room for questions and answers and served as a feedback platform concerning all aspects of the educational program of UbiCrypt.
HackPra Allstars  
(May 21, 2015)

After a one year break, the successful format HackPra Allstars took place in Amsterdam alongside the OWASP AppSec Research 2015 conference. HackPra Allstars happened on May 21, 2015 and presented an interesting compilation of talks from the past Hacker Praktikum sessions. The core focus was set on the field of web-security (and the lack thereof). HackPra Allstars was designed as a conference inside a conference — offering one day with a group of the most interesting figures in today’s web application security and in-security. The OWASP Research 2015 conference provided an ideal framework with around 500 international scholars from all fields of Applied Security.

LightSec 2015  
(September 10-11, 2015)

The LightSec 2015 crypto workshop promoted and initiated novel research on the security and privacy issues for applications that can be termed as lightweight security, due to the associated constraints on metrics such as available power, energy, computing ability, area, execution time, and memory requirements. As such applications are becoming ubiquitous, definitely providing an immense value to the society, they are effecting the public community to a greater extend and leading to a plethora of economical & security and privacy related concerns. The main goal of the workshop was to create a two-day-platform in Bochum where these concerns were addressed and proposed solutions were discussed and evaluated.
Gender & Equality

A very important aim of UbiCrypt is to open the program to all kinds of young researchers. Apart from the equality of the sexes, backgrounds or orientations, the program mainly focuses on practical support.

UbiCrypt offers

- individually shaped part-time PhD options
- child care options during all UbiCrypt events
- an extra quota of travel stipends for female young researchers for each UbiCrypt event
- special funding for female academic collaborations
- individual mentoring

The RUB career service furthermore holds a collaborative equality program supported by all DFG-funded projects at Ruhr-University Bochum. The corresponding round table meets on a regular basis to discuss career development options which specifically suit the needs of young researchers. The program among others includes writing or presentation skills as well as various social skills.

Having hosted the 4th International Workshop on Cryptography, Robustness, and Provably Secure Schemes for Female Young Researchers (CrossFyre) in Bochum in 2014, and this year UbiCrypt will also contribute to CrossFyre 2015 at Radboud University Nijmegen and participate in a panel discussion on Gender & Equality measurements in IT Security related scholarships.
Media offers

UbiCrypt aims to contribute to the popularization of contemporary IT Security. Apart from showing presence at public events or our own regular program offer we constantly inform interested followers about the latest news from our scholars.

The core platform for all current information such as participating scholars, program descriptions, job offers or current calls is our webpage www.ubicrypt.hgi.rub.de.

Our domain at Facebook (www.facebook.com/UbiCrypt) connects international scholars and provides daily updates on the everyday life at our Research Training Group.

Furthermore, some footage of HGI and UbiCrypt events is available on Youtube. Here we present outtakes of conferences and workshops as well as complete lectures to a broader public. These filmic features help to provide an immediate impression of the work at HGI and UbiCrypt and

To best prepare our students for public appearances in the media and to give an overview of current presentation techniques we offered a media coaching with special regard to IT Security topics. The two-day coaching contained writing skills as well as camera training.

We were lucky to contribute to the RUB 50 anniversary movie “SOUND OF RUB”, which ran in local theaters during the celebration week in summer 2015. Our UbiCrypters Prof. Christina Pöpper, Sven Schäge, Carla Ràfols Salvador and Katharina Kohls used the opportunity to talk about their research aims and academic experiences.
Principal Investigators

Prof. Dr. Markus Dürmuth
Mobile Security

Prof. Dr. Sebastian Faust
Applied Cryptography
(since April 2015)

Prof. Dr. Tim Güneysu
Secure Hardware
(until August 2015)

Prof. Dr. Thorsten Holz
Systems Security

Prof. Dr. Eike Kiltz
Cryptography
Principal Investigators

Prof. Dr. Dorothea Kolossa
Digital Signal Processing

Prof. Dr. Gregor Leander
Symmetric Cryptography

Prof. Dr. Kerstin Lemke-Rust
Information Security
(University of Applied Sciences Rhein-Bonn-Sieg)

Prof. Dr. Alexander May
Cryptology

Prof. Dr. Christof Paar
Embedded Security
Principal Investigators

Prof. Dr. Christina Pöpper
Information Security

Prof. Dr. Jörg Schwenk
Network Security | Data Security

Prof. Dr. Hans Ulrich Simon
Mathematics and Computer Science
Postdoctoral Students

Dr. Carla Ràfols Salvador
Public-key Cryptography, Zero-knowledge Proofs
(until September 2015)

Dr. Sven Schäge
Cryptographic authentication and encryption
(since November 2014)
M. Sc. Francesco Aldà
Topic: Privacy-Preserving Learning
Advisors: Prof. Dr. Hans Simon, Prof. Dr. Markus Dürmuth

M. Sc. Christof Beierle
Topic: Design and Analysis of Symmetric Primitives
Advisors: Prof. Dr. Gregor Leander, Prof. Dr. Christof Paar, Prof. Dr. Alexander May

M. Sc. Susanne Engels
Topic: Hardware security --- From Brute-force to Reverse-Engineering
Advisors: Prof. Dr. Christof Paar, Prof. Dr. Kerstin Lemke-Rust, Prof. Dr. Gregor Leander

M. Sc. Maximilian Golla
Topic: Ubiquitous Authentication
Advisors: Prof. Dr. Markus Dürmuth, Prof. Dr. Thorsten Holz, Prof. Dr. Christina Pöpper

M. Sc. Matthias-Franz Horst
Topic: Cryptographic Protocols with TLS Tunnels
Advisors: Prof. Dr. Jörg Schwenk, Prof. Dr. Eike Kiltz
M. Sc. Kai Jansen

Topic: GPS Security
Advisors: Prof. Dr. Christina Pöpper, Prof. Dr. Christof Paar

Dipl.-Math. Elena Kirshanova

Topic: On Complexity of the LWE Problem
Advisors: Prof. Dr. Alexander May, Prof. Dr. Christof Paar

M. Sc. Katharina Kohls

Topic: Steganography and Steganalysis for Multimedia-based Communication Channels
Advisors: Prof. Dr. Christina Pöpper, Prof. Dr. Dorothea Kolossa, Prof. Dr. Thorsten Holz

Dipl.-Inform. Daniel Masny

Topic: Cryptography from Hard Learning Problems
Advisors: Prof. Dr. Eike Kiltz, Prof. Dr. Tim Güneysu

Dipl.-Ing. Hendrik Meutzner

Topic: Acoustic CAPTCHAS for Network Security
Advisors: Prof. Dr. Dorothea Kolossa, Prof. Dr. Thorsten Holz, Prof. Dr. Jörg Schwenk
M. Sc. Jannik Pewny

Topic: Retrofitting Security in Complex Software Systems
Advisors: Prof. Dr. Thorsten Holz, Prof. Dr. Alexander May

M. Sc. Tobias Schneider

Topic: Leakage-Resilient Cryptographic Implementations
Advisors: Prof. Dr. Christof Paar, Prof. Dr. Sebastian Faust, Prof. Dr. Tim Güneysu

M. Sc. Filipp Valovich

Topic: Differential Privacy and Cryptography
Advisors: Prof. Dr. Hans Ulrich Simon, Prof. Dr. Eike Kiltz
M. Sc. Felix Heuer
Topic: Selective Opening secure Public Key Encryption
Advisors: Prof. Dr. Eike Kiltz, Prof. Dr. Alexander May

M. Sc. Thorsten Kranz
Topic: Design and Analysis of Symmetric Primitives in Cryptography
Advisors: Prof. Dr. Gregor Leander

M. Sc. Robert Kübler
Topic: Big Data
Advisors: Prof. Dr. Alexander May

M. Sc. Ilya Ozerov
Topic: Algorithms for Hard Problems
Advisors: Prof. Dr. Alexander May, Prof. Dr. Gregor Leander

M. Sc. Peter Samarin
Topic: Detektion von Plagiaten eingebetteter Software mittels Seitenkanalanalysen
Advisors: Prof. Dr. Christof Paar, Prof. Dr. Kerstin Lemke-Rust
Doctoral Students
(associated collegiates)

M. Sc. Pawel Swierczynski

Topic: Security Aspects of FPGA-Designs and Embedded Software
Advisors: Prof. Dr. Christof Paar, Prof. Dr. Tim Güneysu

Dipl.-Ing. Alexander Wild

Topic: FPGA Security
Advisors: Prof. Dr. Tim Güneysu, Prof. Dr. Hans Ulrich Simon

Qualifying Fellows

B. Sc. Andre Pawlowski

Topic: Large-Scale Analysis of Obfuscated Data
Advisor: Prof. Dr. Thorsten Holz

B. Sc. Friedrich Wiemer

Topic: On the practical hardness of the LWE problem. Implementing BDD enumeration algorithms
Advisor: Prof. Dr. Christof Paar
Dr.-Ing. Christoph Bader

Topic: On the Possibility and Impossibility of Tight Reductions in Cryptography
Advisor: Prof. Dr. Jörg Schwenk

Dr.-Ing. Florian Bergsma

Topic: Modeling an Analyzing Cryptographic Real-World Protocols
Advisor: Prof. Dr. Jörg Schwenk, Prof. Dr. Colin Boyd

Dr.-Ing. Elif Bilge Kavun

Topic: Resource-Efficient Cryptography for Ubiquitous Computing: Symmetric-key Primitives from a Hardware & Software Perspective
Advisor: Prof. Dr. Christof Paar, Prof. Dr. Tim Güneysu

Dr.-Ing. Thomas Pöppelmann

Topic: Efficient Implementation of Ideal Lattice-Based Cryptography
Advisor: Prof. Dr. Tim Güneysu

Dr.-Ing. Felix Schuster

Topic: Securing Application Software in Modern Adversarial Settings
Advisor: Prof. Dr. Thorsten Holz, Prof. Dr. Tim Güneysu, Prof. Dr. Christof Paar
Guests

Dr. Mauro Conti
Associate professor, University of Padua
*Invited Talk HGI Colloquium*

Daniel Bailey
LegacyTexas
*Invited Talk HGI Colloquium*

Prof. Dr. Kaisa Nyberg
Head of Cryptography Group, Aalto University
*Visiting Researcher UbiCrypt*

Prof. Dr. Shai Ben-David
Professor at the School of Computer Science, University of Waterloo
*Invited Talk*

Marie-Sarah Lacharité
Doctoral Researcher, University of Waterloo
*Invited Talk HGI Colloquium*
Guests

Dr. Adela Georgescu
Postdoctoral Researcher, University of Bucharest
Visiting Researcher UbiCrypt

Jan Kopecky
ING Regional IT headquarters
Invited Talk HackPra
Publications by
UbiCrypt (Post)Doctoral Students

Francesco Aldà, Riccardo Aragona, Lorenzo Nicolodi, Massimiliano Sala
Implementation and Improvement of the Partial Sum Attack on 6-Round AES

Christof Beierle, Philipp Jovanovic, Martin M. Lauridsen, Gregor Leander, Christian Rechberger
Analyzing permutations for AES-like ciphers: Understanding ShiftRows

Apostolis Zarras, Katharina Kohls, Markus Dürmuth, Christina Pöpper
Neuralyzer: Flexible Expiration Times for the Revocation of Online Data
ACM conference on Data and Application Security and Privacy (CODASPY) 2016

Marcin Andrychowicz, Daniel Masny, Edoardo Persichetti
Leakage-Resilient Cryptography over Large Finite Fields: Theory and Practice
ACNS 2015

Andrej Bogdanov, Siyao Guo, Daniel Masny, Silas Richelson, Alon Rosen
On the Hardness of Learning with Rounding over Small Modulus
Accepted at TCC2016A

Hendrik Meutzner, Santosh Gupta, Dorothea Kolossa
Constructing Secure Audio CAPTCHAs by Exploiting Differences between Humans and Machines
CHI, Seoul, Korea, April 2015

Malte Darnstädt, Hendrik Meutzner, Dorothea Kolossa
Reducing the Cost of Breaking Audio CAPTCHAs by Active and Semi-Supervised Learning
ICMLA, Detroit, USA, December 2014

Hendrik Meutzner, Viet-Hung Nguyen, Thorsten Holz, Dorothea Kolossa
Using Automatic Speech Recognition for Attacking Acoustic CAPTCHAs: The Trade-off between Usability and Security
ACSAC, New Orleans, USA, December 2014. (Outstanding Paper Award)

Jannik Pewny, Behrad Garmany, Robert Gawlik, Christian Rossow, Thorsten Holz
Cross-Architecture Bug Search in Binary Executables
36th IEEE Symposium on Security and Privacy (Oakland), San Jose, May 2015
Jannik Pewny, Felix Schuster, Lukas Bernhard, Christian Rossow, Thorsten Holz
Leveraging Semantic Signatures for Bug Search in Binary Programs
Annual Computer Security Applications Conference (ACSAC), New Orleans, USA, December 2014

Michael Backes, Thorsten Holz, Benjamin Kollenda, Philipp Koppe, Stefan Nünberger, Jannik Pewny
You Can Run but You Can’t Read: Preventing Disclosure Exploits in Executable Code
21st ACM Conference on Computer and Communications Security (CCS), Scottsdale, Arizona, USA, November 2014

Sven Schäge
TOPAS: 2-Pass Key Exchange with Full Perfect Forward 2015 Secrecy and Optimal Communication Complexity

Tilman Frosch, Sven Schäge, Martin Goll, Thorsten Holz
On Locational Privacy in the Absence of Anonymous Payments 2015
Computers, Privacy & Data Protection (CPDP) 2015 (Junior Scholar Award CPDP 2015)

Felix Heuer, Tibor Jager, Eike Kiltz, Sven Schäge
On the Selective Opening Security of Practical Public-Key 2015 Encryption Schemes

Tibor Jager, Florian Kohlar, Sven Schäge, Jörg Schwenk
Authenticated Confidential Channel Establishment and the 2015 Security of TLS-DHE
Accepted for Journal of Cryptology

Sven Schäge
Tight Security For Signatures Without Random Oracles 2015

Tobias Schneider, Amir Moradi

Tobias Schneider, Amir Moradi, Tim Güneysu

Christoph Bader, Dennis Hofheinz, Tibor Jager, Eike Kiltz, Yong Li
Tightly Secure Authenticated Key Exchange
In Proceedings of the 12th International Conference, TCC 2015

Felix Heuer, Tibor Jager, Eike Kiltz, Sven Schäge
On the Selective Opening Security of Practical Public-Key Encryption Schemes
Public-Key Cryptography -- PKC 2015, Volume 9020 of the series Lecture Notes in Computer Science pp 27-51
Oliver Stecklina, Stephan Kornemann, Felix Grehl, Ramona Jung, Thorsten Kranz, Gregor Leander, Dennis Schweer, Katharina Mollus, Dirk Westhoff
Custom-fit Security for Efficient and Pollution-Resistant Multicast OTA-Programming with Fountain Codes
I4CS 2015, Nuremberg, Germany.

Oliver Stecklina, Peter Langendörfer, Frank Vater, Thorsten Kranz, Gregor Leander
Intrinsic Code Attestation by Instruction Chaining for Embedded Devices
SecureComm 2015, Dallas, USA.

Alexander May, Ilya Ozerov
On Computing Nearest Neighbors with Applications to Decoding of Binary Linear Codes
In Advances in Cryptology (Eurocrypt 2015), Lecture Notes in Computer Science, Springer-Verlag, 2015

James Howe, Thomas Pöppelmann, Máire O’Neill, Elizabeth O’Sullivan, Tim Güneysu
Practical lattice-based digital signature schemes

Tim Güneysu, Vadim Lyubashevsky, Thomas Pöppelmann
Lattice-based signatures: Optimization and implementation on reconfigurable hardware IEEE

Thomas Pöppelmann, Michael Naehrig, Andrew Putnam, Adrián Macías
Accelerating homomorphic evaluation on reconfigurable hardware

Thomas Pöppelmann, Tobias Oder, Tim Güneysu
High-performance ideal lattice-based cryptography on 8-bit ATxmega microcontrollers

Felix Schuster, Manuel Costa, Cédric Fournet, Christos Gkantsidis, Marcus Peinado, Gloria Mainar-Ruiz, Mark Russinovich
VC3: Trustworthy data analytics in the cloud using SGX
In IEEE Symposium on Security and Privacy (S&P), 2015

Felix Schuster, Thomas Tendyck, Christopher Liebchen, Lucas Davi, Ahmad-Reza Sadeghi, Thorsten Holz
Counterfeit object-oriented programming: On the difficulty of preventing code reuse attacks in C++ applications
In IEEE Symposium on Security and Privacy (S&P), 2015

Stephen Crane, Stijn Volckaert, Felix Schuster, Christopher Liebchen, Per Larsen, Lucas Davi, Ahmad-Reza Sadeghi, Thorsten Holz, Bjorn De Sutter, Michael Franz
It’s a TRAP: Table randomization and protection against function reuse attacks
In Proceedings of ACM Conference on Computer and Communications Security (CCS), 2015
Technical Reports
Pawel Swierczynski, Marc Fyrbiak, Phillip Koppe, Christof Paar
FPGA Trojans through Detecting and Weakening of Cryptographic Primitives
IEEE Transactions on Computer-Aided Design of Electronic Systems. 34 (8), 2015

Pawel Swierczynski, Marc Fyrbiak, Christof Paar, Christophe Huriaux, Russell Tessier
Protecting against Cryptographic Trojans in FPGAs

Maik Ender, Gerd Düppmann, Alexander Wild, Thomas Pöppelmann, Tim Güneysu
A Hardware-Assisted Proof-of-Concept for Secure VoIP Clients on Untrusted Operating Systems
2014 International Conference on ReConFigurable Computing and FPGAs, ReConFig14, Cancun, Mexico, December 8-10, 2014, IEEE, 2014, 1-6

Georg Becker, Alexander Wild, Tim Güneysu
Security Analysis of Index-Based Syndrome Coding for PUF-Based Key Generation

Amir Moradi, Alexander Wild
Assessment of Hiding the Higher-Order Leakages in Hardware - What Are the Achievements Versus Overheads?

Alexander Wild, Amir Moradi, Tim Güneysu
Evaluating the Duplication of Dual-Rail Precharge Logics on FPGAs
Talks by UbiCrypt (post)doctoral students

Francesco Aldà
Randomized Response Schemes, Privacy and Usefulness
7th ACM Workshop on Artificial Intelligence and Security with the 21st ACM Conference on Computer Communications Security (CCS), Scottsdale, Arizona, 03.11.-07.11.2014

Christoph Bader
Tightly Secure Authenticated Key Exchange
TCC 2015, Warsaw, Poland, 23.03.-25.03.2015

Christof Beierle
Analyzing Permutations for AES-like Ciphers : Understanding ShiftRows
Krypto-Tag, Paderborn, Germany, 22.01.-23.01.2015

Christof Beierle
Bounding the Differential Probability of SIMON
22. Krypto-Tag, Munich, Germany, 09.07.-10.07.2015

Florian Bergsma
Multi-ciphersuite security of the secure shell (SSH) protocol
CCS 2014, Scottsdale, Arizona, USA, 03.11.-07.11.2014

Felix Heuer
On the Selective Opening Security of Practical Public-Key Encryption Schemes
PKC 2015, Gaitherburg, Maryland, USA, 30.03.-01.04.2015

Thorsten Kranz
On Password Guessing with GPUs and FPGAs
Thorsten Kranz
Cryptanalysis of the ASASA Structure
Krypto-Tag, Paderborn, Germany, 22.01.-23.01.2015

Thorsten Kranz
Integral Attack on the ASASA Block Cipher Construction
Krypto-Tag, Munich, Germany, 09.07.-10.07.2015

Hendrik Meutzner
Constructing Secure Audio CAPTCHAs by Exploiting Differences between Humans and Machines
ACM SIGCHI, Seoul, Korea, 18.04.-23.04.2015

Ilya Ozerov
On Computing Nearest Neighbors with Applications to Decoding of Binary Linear Codes
Workshop: Monthly lattice and crypto meetings, Lyon, France, 25.11.-26.11.2015

Jannik Pewny
Cross-Architecture Bug Search in Binary Executables
IEEE Symposium on Security and Privacy (S&P) 2015, San Jose, California, USA, 18.05.-20.05.2015

Jannik Pewny
Leveraging Semantic Signatures for Bug Search in Binary Programs

Sven Schäge
TOPAS --- 2-Pass Key Exchange with Full Perfect Forward Secrecy and Optimal Communication Complexity
CCS 2015, Denver, Colorado, USA, 12.10.-16.10.2015

Tobias Schneider
Arithmetic Addition over Boolean Masking, Towards First- and Second-Order Resistance in Hardware
13th International Conference on Applied Cryptography and Network Security, New York, USA, 02.06.-05.06.2015

Tobias Schneider
Leakage assessment methodology - a clear roadmap for side-channel evaluations
Tobias Schneider
Leakage Assessment Methodology - a clear roadmap for side-channel evaluations
17th Workshop on Cryptographic Hardware and Embedded Systems, Saint-Malo, France, 13.09.-16.09.2015

Felix Schuster
VC3: Trustworthy Data Analytics in the Cloud using SGX
IEEE Security & Privacy 2015, San Jose, USA, 18.05.-20.05.2015

Pawel Swierczynski
Dissertation project presentation
Hans L. Merkle Foundation presentation day, Essen, Germany, 12.02.-13.02.2015

Pawel Swierczynski
Protecting Against Cryptographic Trojans in FPGAs
IEEE FCCM 2015, Vancouver, Canada, 01.05.-07.05.2015

Alexander Wild
Evaluating the Duplication of Dual-Rail Precharge Logics on FPGAs

Alexander Wild
Security Analysis of Index-Based Syndrome Coding for PUF-Based Key Generation
IEEE International Symposium on Hardware Oriented Security and Trust, Tysons Corner, USA, 05.05.-07.05.2015

Alexander Wild
GliFreD - Glitch-Free Duplication
Krypto-Tag, Munich, Germany, 09.07.-10.07.2015

Alexander Wild
Assessment of Hiding the Higher-Order Leakages in Hardware, what are the achievements versus overheads?
Prof. Dr. Alexander May  
Speaker UbiCrypt  
+49 (0) 234 32 23261  
alex.may@rub.de  

Prof. Dr. Christof Paar  
Deputy Speaker UbiCrypt  
+49 (0) 234 32 22994  
christof.paar@rub.de  

Dr. Dominik Baumgarten  
Coordinator UbiCrypt  
+49 (0) 234 32 29162  
dominik.baumgarten@rub.de  

Dr. Vincent Grosso  
Interdisciplinary Coordinator | Postdoc  
(since January 2016)  
+49 (0) 234 32 29882  
vincent.grosso@rub.de  

Dr. Sven Schäge  
Interdisciplinary Coordinator | Postdoc  
+49 (0) 234 32 29882  
sven.schaege@rub.de
Cryptography is everywhere - PhD and Qualifying Fellowships!

PhD Positions (Full Funding)
We are looking for candidates with outstanding master degrees or diploma from all research fields related to IT-Security.

PhD Positions (Collegiates)
Excellent PhD students with external funding are welcome to join the UbiCrypt doctoral training program.

Qualifying Fellows (Scholarships)
Candidates with excellent bachelor degrees are invited to apply for one-year qualifying scholarships.
Imprint

Editorial Staff
Dominik Baumgarten
Alexander May

Lectorship
Christof Paar
Sven Schäge
Friederike Schneider

Layout
Dominik Baumgarten

Images
Daniel Sadrowski
Roberto Schirdewahn
Dominik Baumgarten

Print
RUB Druckzentrum

Contact
DFG-Research Training Group UbiCrypt
Ruhr-University Bochum
Building ID, 2/150
Universitätsstraße 150
44780 Bochum
Germany

Email: grako@hgi.rub.de
Tel: +49 (0) 234 32 22994
Fax: +49 (0) 234 32 14886
www.ubicrypt.hgi.rub.de
www.facebook.com/UbiCrypt

January 2016

V.i.S.d.P.
Dominik Baumgarten