

Curriculum Vitae

Christopher Wolf

Personal Facts

Date and Place of Birth	7 th of May 1977, Bobingen, Bavaria, Germany
Nationality	German
Marital Status	single, no children
Contact Details	Josephstr. 5, DE-44791 Bochum, Germany chris@Christopher-Wolf.de

Education

January 2003 until November 2005	Ph.D. student at the K.U.Leuven, Belgium
October 1997 until December 2002	Student of computer science at the University of Ulm, Germany, final mark 1.0
October 2001 until September 2002	Student in University College Cork, Ireland
September 1987 until June 1996	Secondary school, leaving certificate with mark 1.3
September 1983 until July 1987	Primary school, leaving certificate with mark 1.33

- Between January 2003 and November 2005, I was a Ph.D. student in the Computer Security and Industrial Cryptography group (COSIC) at the K.U.Leuven (Belgium). My supervisor was Prof. Dr. Ir. Bart Preneel. My thesis is entitled “Multivariate Quadratic Polynomials in Public Key Cryptography”
- In December 2002 I was awarded the degree “Diplom-Informatiker“ (Master's in Computer Science) at the University of Ulm. The overall mark is **1.0** (1.0 is the highest, 5.0 the lowest possible mark). In ECTS notation, this is an “A”. My thesis (6 month individual project work, Supervisors: Prof. Dr Uwe Schöning, University of Ulm, Germany, and Prof. Dr Patrick Fitzpatrick, UCC, Ireland) was entitled “Hidden Field Equations - Variations and Attacks” and marked **1.0**
- I spent my 5th academic year (i.e., October 2001 - September 2002) at University College Cork (Ireland). As there is no ERASMUS exchange between Ulm and Cork, I attended the programme “Master of Science Qualifying in Mathematics”. My overall mark was **80%**, i.e., an “A” in ECTS notation
- I successfully completed the first part of my studies (“Grundstudium“, i.e, the first two

years) in September 1999 with an overall mark of **1.4** (1.0 is the highest, 5.0 the lowest possible mark). In ECTS notation, this is an “A”

- In October 1997 I enrolled at the University of Ulm as a student of computer science
- From September 1987 until June 1996, I attended secondary school at the Justus-von-Liebig-Gymnasium Neusäß (Bavaria, Germany). I completed this studies with an average of **1.3** (1.0 is the highest, 6.0 the lowest possible mark)
- From September 1983 until July 1987, I attended primary school in Diedorf (Bavaria, Germany). My leaving certificate was 1.33 (again, 1.0 is the highest, 6.0 the lowest possible mark)

Languages

- German: *native speaker*
- English: *fluent*
- Dutch: *intermediate level*
- French: *lower intermediate*

Grants

February 2003 until July 2003	Grant of the K.U.Leuven, Belgium
October 2001 until May 2002	Grant of the German Academic Exchange Service (DAAD)

Relevant Working Experience

since May 2007	Scientific Coordinator at the Horst-Görtz Insitute at the Ruhr-University Bochum
October 2006 – April 2007	IT auditor at PricewaterhouseCoopers S.à.r.l. Luxembourg, department for System and Process Assurance (SPA)
December 2005 until September 2006	Post-Doc (<i>Chercheur Post-Doctorant</i>) in the cryptographic research group (<i>Groupe de Cryptographie</i>) in the Department of Informatics at the <i>Ecole Normale Supérieure, 45 rue d'Ulm, Paris (France)</i>

January 2003 until November 2005	Doctoral researcher in the Computer Security and Industrial Cryptography group (COSIC) at the Katholieke Universiteit Leuven (Belgium)
April until June 2001	Student research assistant in the Department of Theoretical Computer Science (<i>Bioinformatics</i>) of the University of Ulm (Germany)
October 2000 until March 2001	Student research assistant in the Department of Theoretical Computer Science (<i>Quantum Computing</i>) of the University of Ulm (Germany)
October 1999 until June 2000	Student teaching assistant for “Theoretical Computer Science” of the University of Ulm (Germany)
August until September 1999	Student teaching assistant for “Exam Preparation Applied Computer Science” of the University of Ulm (Germany)
October 1998 until June 1999	Student Teaching Assistant for “Applied Computer Science” of the University of Ulm (Germany)

Social Year (replacing military service)

September 1996 until September 1997	Full time individual work with disabled people
-------------------------------------	--

Teaching

- Teaching appointment for a lecture on alternative Public Key Systems at the University of Bochum for the summer term 2008
- Seminar Course “Zero Knowledge”: University of Bochum, Germany, October 2004 until March 2005
- Exercise Course “Theoretical Computer Science”: University of Ulm, Germany, October 1999 until June 2000
- Exam Preparation Course “Applied Computer Science”: University of Ulm, Germany, August until September 1999
- Exercise Course “Applied Computer Science”: University of Ulm, Germany, October 1998 until June 1999

Volunteer Activities

- Since July 2004: Founding member of the special interest group for applied cryptology within the “Gesellschaft für Informatik”. Moreover, member of the board of directors in this special interest group with responsibility for the organization of the bi-annual workshop “Kryptotag”. Since September 2006, Chair (“Sprecher”) of the SIG.
- October 1999 until September 2000: Member of the university board (Verwaltungsrat)
- October 1998 until September 2000: President of the students' union and member of the university council Ulm (Senat). In this context, student representative for the introduction of a Bachelor of Arts in Philosophy and a Bachelor of Science / Master's of Science for Multimedia in Computer Science
- October 1998 until June 2001: founding member of the students' parliament (Studierendenvertretung) and the associated society “Trägerverein der Studierendenvertretung e.V.”

Reviewing (Journals)

- IEE Proceedings on Computers and Digital Techniques
- IEEE Transactions on Circuits and Systems I
- IEEE Transactions on Signal Processing
- International Journal of Information Security
- Journal of Computational and Applied Mathematics
- Journal of Symbolic Computation

Conference Organisation

- Eurocrypt 2009 in Cologne, local organizing co-chair
- Western European Workshop on Research in Cryptology (WEWoRC 2007) at the Ruhr-University Bochum, July 4-6, 2007
- International Workshop on Post-Quantum Cryptography (PQCrypto 2006) at the K.U.Leuven, Belgium, May 23-26, 2006.
- Western European Workshop on Research in Cryptology (WEWoRC 2005) at the K.U.Leuven, Belgium, July 5-7, 2005

Board Member

- Australasian Information Security Workshop – Privacy Enhancing Technologies (2006, 2007)
- Kryptographie in Theorie und Praxis (2006, 2007)
- Eurocrypt (2009)
- Post-Quantum Cryptography (2006)
- Sicherheit (2006, 2008)
- Western European Workshop on Research in Cryptology (2005 / co-chair, 2007 / co-chair)

Reviewing (Conferences)

- Africacrypt (2008)
- Applied Cryptography and Network Security (2003)
- Australasian Conference on Information Security and Privacy (2006, 2007)
- Asiacrypt (2004, 2006, 2007)
- Crypto (2004, 2005, 2006, 2007)
- Cryptographers' Track on the RSA conference (2005)
- European Symposium on Research in Computer Security (2004)
- Eurocrypt (2004, 2005, 2006)
- Fast Software Encryption (2007)
- Financial Cryptography (2004)
- Fundamentals of Computation Theory (2005)
- IMA Conference on Cryptography and Coding (2005)
- Indocrypt (2004)
- International Conference on Information Security and Cryptology (2003, 2004, 2007)
- Mycrypt (2005)
- Public Key Cryptography (2005, 2007, 2008)
- Sicherheit (2005, 2006, 2008)
- Western European Workshop on Research in Cryptology (2005, 2007)