



## Dr. Johannes Wolkerstorfer

[Johannes.Wolkerstorfer@xface.at](mailto:Johannes.Wolkerstorfer@xface.at)

Friedrichgasse 29  
8010 Graz, Austria

Mobile +43 681 10291010

[www.linkedin.com/pub/dir/johannes/wolkerstorfer](http://www.linkedin.com/pub/dir/johannes/wolkerstorfer)  
[www.xing.com/profile/Johannes\\_Wolkerstorfer](http://www.xing.com/profile/Johannes_Wolkerstorfer)

## Profile

Dr. Johannes Wolkerstorfer develops systems-on-chip and embedded systems. His focus is on efficient digital hardware and software integration. He gained a lot of experience by researching cryptographic hardware and (co) authored numerous articles in this field. He spread his excellent knowledge about integrating digital hardware in the lectures at Graz University of Technology. From 2010 on, he provides his expertise through the startup company xFace. xFace offers products and services to create sophisticated integrated circuits and embedded systems.

## Personal details

Born: January 12<sup>th</sup> 1973 *Salzburg, Austria*  
Address: Friedrichgasse 29 *Graz, Austria*

## Education

2000–2004	PhD study Computer Science	<i>Telematik, Graz University of Technology</i>
1991–1999	Master study Computer Science	<i>Telematik, Graz University of Technology</i>
1983–1991	Grammar school	<i>Bundesrealgymnasium, Salzburg</i>
1979–1983	Primary school	<i>Salzburg</i>

## Courses

2020	Various	<i>EBS Innovation network, TU Graz</i>
Mar 2016	Agile software testing	<i>RFID qualification network, Expert exchange</i>
Feb 2016	Advanced RFID Lab	<i>RFID qualification network, W. Bösch et.al.</i>
Jan 2016	Agile project management	<i>RFID qualification network, Expert exchange</i>
Nov 2015	Contactless testing	<i>RFID qualification network, M. Gebhart</i>
Sep 2015	EMC on PCB and ICs	<i>RFID qualification network, B. Deutschmann</i>
Mar 2014	Variability in analog circuits	<i>RFID qualification network, M. Pelgrom</i>
Sep 2013	Java for RFID	<i>RFID qualification network, Prof. Slany</i>
May 2013	Advanced analog IC design	<i>RFID qualification network, W. Sansen</i>
Mar 2013	Low-power digital design	<i>RFID qualification network, H. Veendrick</i>
Mar 2013	Agile project management	<i>RFID qualification network, Prof. Slany</i>

## Career

Mar 2010–present Founder and proprietor  
*of xFace – a company creating sophisticated electronic systems* [\[www.xface.at\]](http://www.xface.at)  
Oct 2009–May 2010 Senior researcher  
*at Telecommunications Research Center Vienna (FTW) / Communication Networks*

- Sep 2004–Aug 2009 **Post-doctoral research and teaching assistant**  
*at Graz University of Technology / Institute for Applied Information Processing and  
Communication Technology*
- Sep 2001–Aug 2004 **Research and teaching assistant**  
*at Graz University of Technology / Institute for Applied Information Processing and  
Communication Technology*
- Aug 1998–Aug 2001 **Researcher (third-party funds) for integrated cryptographic circuits**  
*at Graz University of Technology / Institute for Applied Information Processing and  
Communication Technology*
- 1997–1998 **Contracts for services to develop cryptographic circuits**  
*at Graz University of Technology / Institute for Applied Information Processing and  
Communication Technology*
- 1991–1996 **Traineeship and contracts for services in software development, databases  
and information systems**  
*at Siemens PSE Salzburg*

# Experience

## Projects

Johannes Wolkerstorfer contributed to many national and international projects

- 2020 HW & SW design of a FPGA card with PCIe interfacing secure elements  
Customer: Yagoba GmbH
- 2020 Horizon 2020 project evaluation (Expert on ICT)  
Customer: European Commission
- 2019 Digital design of a mixed-signal IC of an audio DAC and amplifier  
Customer: ams AG
- 2018 – 2019 Design and integration of a 32-bit audio DSP on 40nm CMOS  
Customer: ams AG
- 2017 – 2018 Concept and FPGA prototyping of an audio signal processor  
Customer: ams AG
- 2016 – 2017 System verification of a mixed-signal audio chip set  
Customer: ams AG
- 2015 – 2016 Mixed-signal evaluation of a smart power switch  
Customer: ams AG
- 2015 – 2017 FP7 project evaluation (Innovation expert for Internet-of-Things)  
Customer: European Commission
- 2015 Test environment for Javacard applets  
Customer: Yagoba GmbH
- 2014 – 2015 Optimization of a digital circuit for power-management ICs  
Customer: ams AG
- 2014 Sequence and non-volatile controller for power-management ICs  
Customer: ams AG
- 2014 Innovation expert for project in the Internet of things  
Review of FP7 Strep project for EU commission
- 2014 Cryptographic library for Javacard applets  
Customer: Yagoba GmbH
- 2014 Digital design of a novel rotary encoder chip  
Customer: ams AG
- 2013 – 2014 Digital design of ACPI-compliant power management chip  
Customer: ams AG
- 2013 Consulting: Patent analysis and prior art retrieval  
Prior art of public-key co-processors (RSA, DH, elliptic-curve)
- 2013 Genuine hardware authentication and encrypted firmware update  
Customer: AVL
- 2013 Digital design of a novel tracking ADC for rotary encoders  
Customer: ams AG
- 2013 Digital design of complex power management chip  
Customer: ams AG
- 2013 Digital design of a rotary encoder chip  
Digital design including synthesis and design for test. Signal processing and secure IO.  
Customer: ams AG
- 2013 Production test for an optical Gigabit interface applied in aviation  
Customer: AviBit GmbH
- 2012 Digital design of a rotary encoder chip

- Digital design including synthesis and design for test. Signal processing.  
Customer: ams AG
- 2012 **Security concept for RFID-based transport card**  
Customer: Identec Solutions GmbH
- 2012 **Jitter measurement of optical SFP modules**  
Customer: AviBit GmbH
- 2011 – 2012 **Digital design of complex power management chip**  
Customer: austriamicrosystems AG
- 2011 – 2012 **FPGA Board for network monitoring (1G and 10G Ethernet)**  
Custom FPGA board with eight 1G Ethernet interfaces (SFP) and one 10G interface. Main contractor for concept, board production, digital design, embedded software, and startup.  
Customer: Telecommunications Research Center Vienna FTW
- 2011 **Encrypted firmware update**  
Encrypted firmware update for read-protected DSP controllers (TI C2000 TMS320F28x).
- 2011 **Microphone array**  
FPGA based microphone array for capturing 32+ audio channels (24 bit, 192 kHz), UDP based protocol for transmission, AES3/EBU (SPDIF) digital output.  
Customer: Joanneum Research
- 2011 **Digital interface for sensor chip**  
Integration of I2C (high-speed), SPI, and OTP memory for rotary encoder.  
Customer: austriamicrosystems AG
- 2011 **FPGA demonstrator for network monitoring**  
Capturing of Gigabit network data of optical backbones in mobile communication (SFP interface, GPS time tagging, data aggregation, flow identification, UDP protocol).  
Customer: Telecommunications Research Center Vienna FTW
- 2010 – 2012 **Non-coherent orthogonal frequency division multiplexing (Fit-IT project NOFDM)**  
FPGA-based digital hardware platform with PC/Matlab connectivity and hardware implementation of DSP algorithms.  
Partners: TU Graz SPSC, EPCOS (TDK), Xerxes Technology, xFace
- 2010 **Digital design of two mixed-signal chips**  
Digital circuit for power-management chips: Verilog RTL (multi clock domain, clock gating), functional verification.  
Customer: austriamicrosystems AG
- 2009 – 2010 **Privacy-aware Secure Monitoring (European FP7 project PRISM)**  
Digital hardware for threshold cryptography and bulk encryption on NetFPGA (Xilinx FPGA)  
Partners: FTW, Fraunhofer, ETH Zürich, CNIT (Rome, Pisa), Hitachi, ...
- 2008 – 2009 **Cryptographic Protected Tags for new RFID Applications (Fit-IT project CRYPTA)**  
Requirement definition and flexible tag architecture for cryptographic enhanced RFID tags  
Partners: IAIK, Austriamicrosystems, RF-IT
- 2006 – 2007 **Programme for Advanced Contactless Technologies PROACT (teaching and research programme funded by NXP semiconductors)**  
Coordinator of the programme. Organization of RFID summerschools, coordination of core research group: secure RFID  
Partners: NXP Semiconductors, Institutes of Graz University of Technology (IAIK, IFE, ITI, INW, IBK, EMT)
- 2005 – 2008 **Quantum Cryptography on Chip (Fit-IT project QCC)**  
Technical lead of TU Graz contribution: 1 Gbps IPsec encryption engine with Linux integration and management interface on a Xilinx Virtex-4 board  
Partners: IAIK, ARC, Siemens
- 2004 – 2005 **Authentication for long-range RFID Technology (Fit-IT project ART)**

- Development of the smallest AES encryption engine “Tina” realized on 0.35  $\mu\text{m}$  CMOS using standard cells.  
Partners: IAIK, NXP Semiconductors, FH Joanneum, Siemens
- 2004 **PhD thesis “Hardware Aspects of Elliptic-Curve Cryptography”**  
Study how ECC can be implemented efficiently in resource constricted devices and how ECC can be accelerated by hardware
- 2002 – 2004 **Elliptic Curve Crypto Unit ECCU**  
Dual-field elliptic curve crypto unit for resource constricted devices
- 2002 **PCI-Card for Accelerating ECC over  $\text{GF}(2^m)$  FASTGF2**  
Low-cost solution to accelerate ECC over  $\text{GF}(2^m)$  on FPGA cards significantly
- 2001 **AES - submodule design for smart card AES**  
32-bit architecture for the Advanced Encryption standard plus efficient approaches to implement the Sboxes and MixColumns function in hardware
- 2000 **High speed VLSI controller including CRT for RSA (FWF project RSAj)**  
Full-custom design of a programmable controller for RSA exponentiation
- 1998 – 2000 **High speed VLSI triple-DES-module (EU project SCAN)**  
Design and implementation of 155 Mbit/s Triple-DES encryption engine on a 0.6  $\mu\text{m}$  CMOS technology using full-custom design: true-single phase logic  
Partners: IAIK, Robotica
- 1999 **Master Thesis “High Speed VLSI Triple-DES-Module”**  
Design rationale of a full-custom optimized encryption core
- 1996 **Students project at IAIK: DES und TRIPLE DES auf XILINX**  
Resource optimized triple DES core for Xilinx FPGA
- 1991 – 1996 **Software development for Siemens PSE**  
Implementation of databases for public services

## Teaching

At his time at TU Graz, Johannes serviced up to 200 students per semester.

- 2002 – 2009 **“VLSI Design VO” lecture at Graz University of Technology**  
Lecture for about 30 students per semester about the structured approach to integrate digital circuits in CMOS technology.
- 2001 – 2009 **“VLSI Design KU” lab exercise at Graz University of Technology**  
Lab exercise for about 30 students per semester where a cryptographic circuit has to be implemented as integrated circuit (ASIC). It comprehends system specification, high-level model, HDL model, synthesis, place and route, backend verification, netlist extraction and power simulation. Used tools are from Cadence, Mentor Graphics, and Synopsys.
- 2007 – 2009 **“System-on-Chip Architectures and Modeling VU” integrated lecture and lab at Graz University of Technology**  
Project oriented lecture where roughly 10 students build a system on chip. E.g. in 2008 a networked long-range RFID reader (analog frontend, digital frontend, bus interface to processor, Linux drivers, webservice, demo application).
- 2006 – 2009 **“Rechnernetze und Organisation VO” lecture at Graz University of Technology**  
Introductory lecture for roughly 175 students of Software engineering with two topics: computer organization (processor, instruction sets, components) and computer networks (Ethernet, IP)
- 2006 – 2009 **“Rechnernetze und Organisation KU” lab exercise at Graz University of Technology**  
Lab exercise for about 175 students of software engineering: x86 assembler, x86 instruction set simulation, network simulation or analysis. Used programming language: C/C++
- 2002 – 2009 **Advisor and assessor of master theses for the study Telematik at Graz University of Technology**  
See below
- 2001 – 2009 **Advisor of master projects for the study Telematik at Graz University of Technology**

- Medium-sized projects on FPGA demo boards
- 2004 – 2009 Advisor of bachelor projects for the study Telematik at Graz University of Technology
- Small projects on FPGA demo boards and seminar paper
- 2008 “Requirements, Algorithms, Architectures -- The design space of ECC hardware” at BCRYPT ECC-Day 20 Mar 2008, Louvain-la-Neuve, Belgium.
- 2008 “Introduction to RFID Security” at PROACT Springschool on RFID 2008, Graz, Austria
- 2007 Organization of “PROACT Springschool on RFID 2007”, 18-20 April 2007, Graz.
- 2006 Organization of “PROACT Summerschool on RFID 2006”, 10-12 July 2006, Graz.
- 2006 “Secret Key Building Blocks”, Summer School on Cryptographic Hardware, Side-Channel and Fault Attacks (EcryptSS06), Louvain-la-Neuve, June 2006.
- 2004 “Authentication with RFID Tags”, Intensive Program on Information and Communication Security: Secure Embedded Systems - IPICS 2004, Graz.

### Program committees and scientific reviews

Johannes is program committee member of the international CHES conference, which is the flagship conference for cryptographic hardware. In 2007, he organized the national Austrochip workshop in Graz (1 day, 100 visitors) and published its proceedings.

- 2001 – 2020 Austrochip Program committee member of Austrochip Workshop on Microelectronics
- 2008 – 2009 CHES Program committee member of Cryptographic Hardware and Embedded Systems
- 2009 FDDC Program committee member of Workshop on Fault Diagnosis and Tolerance in Cryptography
- 2008 CARDIS Program committee member of Cardis
- 2008 CSNDSP Local committee of Communication Systems, Networks and Digital Signal Processing CSNDSP
- 2007 Austrochip General chair of Austrochip Workshop on Microelectronics 2007
- 2007 RFID Program committee member of 1st International EURASIP Workshop on RFID Technology RFID
- 2006 RFIDsec Program committee member of Workshop on RFID Security
- 2002 CHES External referee of Cryptographic Hardware and Embedded Systems CHES

### Assessor (Begutachter) of master theses

- 2009 Johann Ertl, “Security Enhanced UHF RFID Digital Controller ASIC”
- 2008 Daniel Hein, “Elliptic Curve Cryptography ASIC for Radio Frequency Authentication”
- 2008 Michael Hofmann, “FPGA extension for a chip card test device with an interface for the single wire protocol”
- 2008 Andreas Auer, “Scaling Hardware for Electronic Signatures to a Minimum - A Low-Power Elliptic Curve Processor”
- 2008 Georg Hofferek, “Exploring the Design Space of the GPS Authentication Scheme”
- 2007 Johannes Loinig, “Gigabit Packet Filtering on Configurable Hardware”
- 2007 Stefan Lemsitzer, “Multi-Gigabit Authenticated Encryption Core Optimized for FPGAs and ASICs”

### Advisor (Betreuer) of master theses

- 2007 Christoph Bouvier, “Evaluation of Distributed Management Approaches for Embedded Systems”
- 2006 Franz Fürbass, “ECC Processor with Low Die Size for RFID Applications”

- 2005 Christian Pühringer, "High Speed Elliptic Curve Processor: An Implementation of the Elliptic Curve Digital Signature Algorithm (ECDSA) over GF(p) in hardware on an FPGA PCI Board"
- 2005 Thomas Wöckinger, "High-Speed RSA Implementation for FPGA Platforms"
- 2003 Harald Aigner, "Parallelized Co-processor for Elliptic Curve Cryptography and its Embedding in a System on Chip"
- 2003 Martin Feldhofer, "Controlling Smart Tags"
- 2002 Stefan Stampfer, "Timing Verification of a Modular Hardware Design"

## Publications

### Conference proceedings

- 2011 Michael Hutter, Martin Feldhofer, Johannes Wolkerstorfer, "A Cryptographic Processor for Low-Resource Devices: Canning ECDSA and AES like Sardines", Proceedings of Workshop in Information Security Theory and Practice - WISTP 2011
- 2010 Johannes Wolkerstorfer, "Secret-Sharing Hardware Improves the Privacy of Network Monitoring", Proceedings of 5<sup>th</sup> International Workshop on Data Privacy Management (DPM) 2010, Springer LNCS 6514 pp. 51-63.
- 2010 Giuseppe Bianchi, Johannes Wolkerstorfer, Simone Teofili, Ivan Gojmerac, Oliver Jung "Feasibility of Wire-Speed Hardware-based Conditional Per-flow Encryption for On-the-Fly Protection of Monitored Traffic", Proceedings of Mobile Summit 2010
- 2009 Michael Hutter, Alexander Szekely, Johannes Wolkerstorfer "Embedded System Management using WBEM", Proceedings of Integrated Network Management - IM2009
- 2009 Michael Hutter, Marcel Medwed, Daniel Hein, Johannes Wolkerstorfer "Attacking ECDSA-Enabled RFID Devices", Proceedings of Applied Cryptography and Network Security – ACNS 2009
- 2008 Georg Hofferek, Johannes Wolkerstorfer "Coupon Recalculation for the GPS Authentication Scheme", Proceedings of Smart Card Research and Advanced Applications – CARDIS 2008
- 2008 Thomas Lorünser, Edwin Querasser, Thomas Matyus, Momtchil Peev, Johannes Wolkerstorfer, Michael Hutter, Alexander Szekely, Ilse Wimberger, Christian Pfaffel-Janser, Andreas Neppach "Security Processor with Quantum Key Distribution", Proceedings of Application-Specific Systems, Architectures and Processors – ASAP 2008
- 2008 Daniel Hein, Johannes Wolkerstorfer, Norbert Felber "ECC is Ready for RFID – A Proof in Silicon", Informal Proceedings of RFIDsec 2008
- 2008 Andreas Neppach, Christian Pfaffel-Janser, Ilse Wimberger, Thomas Lorünser, Michael Meyenburg, Alexander Szekely, Johannes Wolkerstorfer "Key Management of Quantum Generated Keys in IPsec", Proceedings of Secrypt 2008
- 2008 Johannes Wolkerstorfer, Alexander Szekely, Thomas Lorünser "IPsec Security Gateway for Gigabit Ethernet", Proceedings of Austrochip 2008
- 2008 Daniel Hein, Johannes Wolkerstorfer, Norbert Felber "ECC is Ready for RFID – A Proof in Silicon", Proceedings of SAC 2008
- 2007 Franz Fürbass, Johannes Wolkerstorfer "ECC Processor with Small Footprint for RFID Applications", Proceedings of IEEE Circuits and Systems – ISCAS 2007
- 2007 Stefan Lemsitzer, Johannes Wolkerstorfer, Norbert Felber, Matthias Brändli "Multi-Gigabit GCM-AES Architecture Optimized for FPGAs", Proceedings of Workshop on Cryptographic Hardware and Embedded Systems 2007 – CHES 2007
- 2007 Martin Feldhofer, Johannes Wolkerstorfer "Strong Crypto for RFID Tags - a Comparison of Low-Power Hardware Implementations" Proceedings of IEEE Circuits and Systems – ISCAS 2007
- 2007 Johannes Loinig, Johannes Wolkerstorfer, Alexander Szekely "Packet Filtering in Gigabit Networks Using FPGAs", Proceedings of Austrochip 2007
- 2006 Manuel Koschuch, Joachim Lechner, Andreas Weitzer, Johann Großschädl, Alexander Szekely, Stefan Tillich, Johannes Wolkerstorfer "Hardware/Software Codesign of Elliptic Curve Cryptography on an 8051 Microcontroller", Proceedings of Cryptographic Hardware and Embedded Systems – CHES 2006
- 2005 Norbert Pramstaller, Stefan Mangard, Sandra Dominikus, Johannes Wolkerstorfer "Efficient AES Implementations on ASICs and FPGAs", Proceedings of Advanced Encryption Standard – AES04
- 2005 Martin Feldhofer, Johannes Wolkerstorfer "Low-power Design Methodologies for an AES Implementation in RFID Systems", Workshop on Cryptographic Advances in Secure Hardware – CRASH 2005
- 2005 Johannes Wolkerstorfer "Scaling ECC Hardware to a Minimum", Proceedings of Austrochip 2005
- 2005 Christian Pühringer, Johannes Wolkerstorfer "High Speed Elliptic Curve Cryptography Processor for GF(p)", Proceedings of Austrochip 2005

- 2004 Harald Aigner, Holger Bock, Markus Hütter, Johannes Wolkerstorfer "A Low-Cost ECC Coprocessor for Smartcards", Proceedings of Cryptographic Hardware and Embedded Systems – CHES 2004
- 2004 Norbert Pramstaller, Johannes Wolkerstorfer "A Universal and Efficient AES Co-processor for Field Programmable Logic Arrays", Proceedings of Field-Programmable Logic and Applications – FPL 2004, LNCS 3203
- 2004 Martin Feldhofer, Sandra Dominikus, Johannes Wolkerstorfer "Strong Authentication for RFID Systems using the AES Algorithm", Proceedings of Cryptographic Hardware and Embedded Systems – CHES 2004
- 2003 Norbert Pramstaller, Johannes Wolkerstorfer "An Efficient AES Implementation for Re-configurable Devices", Proceedings of Austrochip 2003
- 2003 Wolfgang Bauer, Johannes Wolkerstorfer "Hochleistungs-ECC mit Standardkomponenten", Proceedings of the 8. BSI-Kongress für IT-Sicherheit – BSI 2003
- 2002 J. Wolkerstorfer "Dual-Field Arithmetic Unit for GF(p) and GF(2<sup>m</sup>)", Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems – CHES 2002, LNCS 2523
- 2002 J. Wolkerstorfer, E. Oswald, M. Lamberger "An ASIC implementation of the AES SBoxes", Proceedings of the Cryptographer's Track at the RSA Conference – RSA 2002, LNCS 2271
- 2002 J. Wolkerstorfer, W. Bauer "A PCI-Card for Accelerating Elliptic Curve Cryptography", Proceedings of Austrochip 2002
- 2001 Johannes Wolkerstorfer "An ASIC implementation of the AES-MixColumns operation", Proceedings of Austrochip 2001
- 2000 R. Ingruber, H. Leitold, W. Mayerwieser, U. Payer, K.C. Posch, R. Posch, J. Wolkerstorfer "ISDN Channel Security Demonstration Board", Proceedings of 2<sup>nd</sup> International Network Conference, INC 2000, pp. 297-304, ISBN: 1-84102-066-4.
- 2000 H. Leitold, W. Mayerwieser, U. Payer, K.C. Posch, R. Posch, J. Wolkerstorfer "A 155 Mbps triple-DES network encryptor", Proceedings of CHES 2000, LNCS 1965, pp. 163–173
- 2000 H. Leitold, W. Mayerwieser, U. Payer, K.C. Posch, R. Posch, J. Wolkerstorfer "Robustness-Agile Encryptor for ATM Networks", Proceedings of IFIP SEC 2000, ISBN 0-7923-7914-4, pp. 231-240
- 1999 H. Leitold, W. Mayerwieser, U. Payer, K.C. Posch, R. Posch, J. Wolkerstorfer "Single Chip Key-Agile ATM Encryptor", Proceedings of Austrochip 1999, pp. 109-116

## Journal articles

- 2007 Johannes Wolkerstorfer, Karl Hollaus "PROACT: RFID-Impulse an der TU Graz", e&i – ÖVE-Verbandzeitschrift Elektrotechnik und Informationstechnik
- 2005 Martin Feldhofer, Johannes Wolkerstorfer, Vincent Rijmen "AES Implementation on a Grain of Sand", IEE proceedings / information security (Volume: 152)

## Book chapter

- 2008 Martin Feldhofer, Johannes Wolkerstorfer "Hardware Implementation of Symmetric Algorithms for RFID Security" in "RFID Security: Techniques, Protocols and System-On-Chip Design", Springer, ISBN: 978-0-387-76480-1

## Book editor

- 2007 Johannes Wolkerstorfer, Karl-Christian Posch – "Proceedings of Austrochip 2007" – Proceedings, Verlag der Technischen Universität Graz, ISBN: 978-3-902465-87-0

## PhD thesis, master thesis

- 2004 Johannes Wolkerstorfer "Hardware Aspects of Elliptic Curve Cryptography", PhD thesis, Graz University of Technology
- 1999 Johannes Wolkerstorfer "High Speed VLSI Triple-DES-Module", Master thesis, Graz University of Technology

## Other things

- Languages: German, English
- Driving license: A (motorcycle), B (cars)
- Family: Two kids: Alex (Nov 2005) and Thomas (May 2009)
- Hobbies: Family, biking (race & mtb), swimming, hiking, wine (red & white), travelling