

Curriculum Vitae

Last Update: 6.3.2018

Personal Information

Name:	Dipl.-Ing. Dr. techn. Pacher Christoph
Nationality:	Austrian
Date of birth:	16.8.1974

Education and Training

Dates (from – to)	Name and type of the organisation	Principal subjects	Title awarded
04/13 – 05/13	University of South Australia, Institute for Telecommunications Research (Visiting researcher)	Communication Theory	
09/11 - 10/11	ETH Zürich, Institute of Theoretical Physics (Visiting researcher)	Quantum Information Theory	
1999 - 2007	TU Wien, Institute of Solid State Electronics	Semiconductor Electronics / Quantum Physics Thesis " <i>Engineering of Electronic Properties of Finite Periodic Quantum Structures</i> " Supervisor: Prof. E. Gornik	Dr. techn.
1993 - 1999	TU Wien, Faculty of Electrical Engineering	Electrical Engineering / Computer Technology Thesis „ <i>Untersuchung von Übergittertransport für THz- Quellen</i> “ (Semiconductor Physics) at Institute of Solid State Electronics	Dipl.-Ing.
1993 – 1996	TU Wien, Faculty of Computer Science	Computer Science	
1988 - 1993	Technical High School TGM - Technologisches Gewerbemuseum HTBLuVA Wien XX	Communication Engineering	

Work Experience

Dates (from – to)	Name and type of the employer	Position held	Main activities and responsibilities
2004 – ongoing	AIT Austrian Institute of Technology GmbH (formerly Austrian Research Centers)	Senior Scientist (since 2018) / Scientist (before 2018)	<p>Scientific lead, post processing algorithms for quantum cryptographic protocols</p> <ul style="list-style-type: none"> - expanding and intensifying the cont(r)acts with the international scientific network of AIT and the European industry - lecturer at scientific workshops at conferences and research institutes - developing statistical methods for error estimation - analysing and fixing vulnerabilities of authentication algorithms - optimization of information reconciliation algorithms and authentication algorithms - developing efficient numerical algorithms based on finite fields - adaption of algorithms to satellite-based quantum key distribution (QKD) - supervising a PhD student jointly with Technical University of Denmark <p>Scientific lead, theoretical aspects of quantum cryptography</p> <ul style="list-style-type: none"> - expanding and intensifying the cont(r)acts with the international scientific network of AIT - proving the information-theoretic (statistic) security of particular QKD protocols and quantum random number generators (QRNG) - modelling of the AIT continuous-variable QKD system (quantum optics plus technical noise sources) - modelling of QRNGs - supervising student in pre diploma project work at TU Wien

			<p>Administrative responsibilities</p> <ul style="list-style-type: none"> - Project management of national and international research projects in the field of quantum cryptography - Developing research ideas, coordinating and authoring of research proposals - business acquisition for AIT QKD post processing software - Patent researches - Participating in standardization (ETSI, IEEE) - Mentoring summer students - Organisation of scientific workshop in Vienna <p>Technical responsibilities</p> <ul style="list-style-type: none"> - Implementing high performance algorithms for the AIT QKD software library - First contact for IT related issues in the business unit - Developing high performant software for the numerical simulations of optoelectronic devices (until 2008)
1999-2003	TU Wien	Research Assistant	<ul style="list-style-type: none"> - Experimental study of hot electron transport in III-V semiconductor hetero-structures (processing of samples in clean room, measuring at liquid helium temperature) - Theoretical study of quantum mechanical tunnelling through periodic (hetero)structures - supervision of two diploma students - supervision of several students “cleanroom work” (8 credit hours each)

1995-1998	TU Wien	Teaching Assistant (Tutor)	Teaching - Communication Engineering UE (2 credit hours) - Exercises Mathematics 3 for electrical engineering (1.5 credit hours) - Exercises Mathematics 2 for electrical engineering (2 credit hours) - Exercises Mathematics 1 for electrical engineering (3 credit hours)
1994–2001	Self-employed working for Alcatel AG, Vienna Fenböck Umwelttechnik, Strasshof	Software Engineer	- Development and implementation of software for an embedded system communicating via short messages (SMS) - Programming of logic controller for sewage plant

Languages

Language	Reading / writing / verbal	Level (basic, good, excellent)
German	✓ / ✓ / ✓	Mother tongue
English	✓ / ✓ / ✓	Excellent

Technical skills ((software-)tools, machinery, equipment, etc.)

Technical skill	Level (basic, good, excellent)
MS Office	Excellent
LaTeX typesetting system	Excellent
Wolfram Mathematica	Excellent
Matlab	Good to Excellent
Programming Languages (C++14, C, Python, Pascal, Assembler)	Good to Excellent
Development Tools (SVN, Git, Redmine, CMake, GCC, GDB, GPROF,...)	Good to Excellent
Linux system administration (Debian)	Good
Parallel programming frameworks (MPI, OpenMP, OpenCL)	Basic to Good
Processing of semiconductor hetero-structures in clean room (positive and negative lithography, wet-chemical etching, metal evaporation and sputtering, reactive ion etching)	Good
Analysis of semiconductor hetero-structures at room temperature and liquid helium temperature	Good

Selected Publications (numbering according to separate list of publications)

- J28 M. Tomamichel, J. Martinez-Mateo, **C. Pacher**, D. Elkouss, Fundamental finite key limits for one-way information reconciliation in quantum key distribution, *Quantum Information Processing* 16, 280, 2017.
- P17 **C. Pacher**, P. Grabenweger, D.E. Simos, Weight distribution of the syndrome of linear codes and connections to combinatorial designs, *IEEE International Symposium on Information Theory – Proceedings 2016*, 3038-3042, 2016.
- J27 **C. Pacher**, A. Abidin, T. Lorünser, M. Peev, R. Ursin, A. Zeilinger, Larsson, J.-A., Attacks on quantum key distribution protocols that employ non-ITS authentication, *Quantum Information Processing* 15, 327-362, 2016.
- J25 T. Gehring, V. Händchen, J. Duhme, F. Furrer, T. Franz, **C. Pacher**, R. F. Werner, R. Schnabel, Implementation of continuous-variable quantum key distribution with composable and one-sided-device-independent security against coherent attacks, *Nature Communications* 6, 8795, 2015.
- P16 **C. Pacher**, P. Grabenweger, J. Martinez-Mateo, V. Martin, An information reconciliation protocol for secret-key agreement with small leakage, *IEEE International Symposium on Information Theory – Proceedings 2015*, 730-734, 2015.

- J24 M. Valle, H. Schabauer, **C. Pacher**, H. Stockinger, A. Stamatakis, M. Robinson-Rechavi, N. Salamin, Optimization strategies for fast detection of positive selection on phylogenetic trees, *Bioinformatics* 30, 1129-1137, 2014.
- J23 Lechner, **C. Pacher**, Estimating channel parameters from the syndrome of a linear code, *IEEE Communications Letters* 17, 2148-2151, 2013.
- J21 Windhager, M. Suda, **C. Pacher**, M. Peev, Poppe, A., Quantum interference between a single-photon Fock state and a coherent state, *Optics Communications* 284, 1907-1912, 2011.
- J19 M. Peev, **C. Pacher**, et.al., The SECOQC quantum key distribution network in Vienna, *New Journal of Physics* 11, 075001, 2009.
- Pat1 N. Finger, **C. Pacher**, European patent EP2051138: Device for generating polarisation-entangled photons, 2009.
- J14 **C. Pacher**, W. Boxleitner, E. Gornik, Coherent resonant tunneling time and velocity in finite periodic systems, *Physical Review B* 71, 1253171 – 1253181, 2005.
- J10 **C. Pacher**, E. Gornik, Adjusting the coherent transport in finite periodic superlattices, *Physical Review B* 68, 155319, 1-9, 2003.
- J4 M. Kast, **C. Pacher**, G. Strasser, E. Gornik, W.S.M. Werner, Wannier-Stark states in finite superlattices, *Physical Review Letters* 89, 136803, 1-4, 2002.

Awards & Scholarships

- In 2010, scholarship for participation in the “Advanced School in Quantum Information Processing and Quantum Cryptography” in Montreal
- In 2010, award for successful participation in the ICT Call of Wiener Wissenschafts-Forschungs- und Technologiefonds
- In 2007, academic degree Dr. techn. with highest distinction
- In 1999, academic degree Dipl.-Ing. with highest distinction

Memberships and Functions

- Member IEEE Information Theory Society
- Member IEEE Communications Society
- Member ETSI Industry Specification Group in Quantum Key Distribution
- Reviewer for Nanoscale Research Letters, Quantum Information & Computation, Quantum Information Processing, Science Reports, Swiss National Science Foundation, International Conference on Quantum Cryptography, IEEE International Symposium on Information Theory
- Co-organizer and TPC co-chair of International QKD Post Processing Workshop 2011 in Vienna