

name Prof. dr. ir. Bart Preneel

POSITION Full Professor at KU Leuven, Belgium

WORK EXPERIENCE

- 2000-present **Full Professor KU Leuven**
(associate professor 2000-2003, professor 2003-2005).
Head of COSIC research group since 2013
[Business or sector](#) academia
- 2021-present **Board member of Approach**
Cybersecurity services and solutions company
[Business or sector](#) cybersecurity
- 2019-present **Founder and Board member nextAuth**
Startup in mobile authentication
[Business or sector](#) cybersecurity
- 2005-2011 **Scientific advisor**
Philips Research, Eindhoven, The Netherlands
[Business or sector](#) semiconductor and consumer electronics
- 1999-2000 **Research Associate at KU Leuven (funded by FWO)**
FWO Flanders and KU Leuven, Belgium
[Business or sector](#) academia
- 1993-1999 **Postdoctoral Researcher at KU Leuven (funded by FWO)**
FWO Flanders and KU Leuven, Belgium
[Business or sector](#) academia
- 1993-1994 **Research Fellow**
University of Berkeley at California, USA
[Business or sector](#) academia
- 1987-1993 **Research Assistant at KU Leuven (funded by FWO)**
FWO Flanders and KU Leuven, Belgium
[Business or sector](#) academia

EDUCATION AND TRAINING

- 1987-1993 **Doctoral Degree in Engineering (summa cum laude)** PhDt
Doctorate in Cryptography at KU Leuven, Belgium
▪ cryptography, information theory, coding theory
- 1982-1987 **Master of Electrical Engineering (summa cum laude)** MSc (burg. ir.)
KU Leuven, Belgium
▪ signal processing, digital and analog communications, chip design, control theory
- 1986-1987 **Economics**

KU Leuven, Belgium

- program equivalent to BSc in economics that gives access to MSc in economics

1975-1981

High School

Sint-Pieterscollege, Leuven, Belgium

- Latin-Greek

PERSONAL SKILLS

Mother tongue(s)

Dutch

Other language(s)

	UNDERSTANDING		SPEAKING		WRITING
	Listening	Reading	Spoken interaction	Spoken production	
English	C2	C2	C2	C2	C2
French	C2	C2	C2	C1	C1
German	C1	C1	C1	B2	B1

Levels: A1/A2: Basic user - B1/B2: Independent user - C1/C2 Proficient user
[Common European Framework of Reference for Languages](#)

Communication skills

- excellent communication skills gained through scientific writing, teaching and project management; regularly quoted as expert in Belgian and international media

Organisational / managerial skills

- leadership: currently responsible for a research team of 100 people. Six years experience as President of the IACR (International Association for Cryptologic Research), a scientific association with more than 1500 members. More than 15 years experience as President of LSEC, an international association that brings together 70 companies and research labs in cyber security. Project coordinator of 8 EU projects.

ADDITIONAL INFORMATION

Publications	More than 100 international journal publications, more than 400 international conference publications, editor of 28 books and 5 international standards
Presentations	Keynote lecturer or invited speaker at more than 130 conferences or schools in 50 countries (including Asiacrypt, Eurocrypt, Esorics, IFIP SEC, FSE, PKC, CHES and several ENISA Summer Schools).
Supervision	Graduated 70 PhD students and supervision of 50 postdoctoral researchers; currently supervising 14 PhD students
Projects	Project manager of 8 EU projects (30 MEUR total budget) and participant in more than 40. Joint manager of strategic research program Cybersecurity Initiative Flanders (8 MEUR/year).
Conferences	General chair of 3 international conferences, program chair of more than 20 conferences including Eurocrypt, ESORICS, Financial Cryptography and Data Security, Indocrypt, ACNS, Annual Privacy Forum. Director of two NATO Advanced Research Workshops; program committee member for more than 250 conferences
Journals	Founding editor in chief of Transactions on Symmetric Cryptology; served as member of the editorial board of the Journal of Computer Security, ACM Transaction on Information Security, IEEE Transactions on Information Forensics and Security, International Journal of Information & Computer Security, Cryptologia
Honours and awards	Visiting professor at the Technical University of Denmark, TU Graz (Austria), University College London (UK), University of Bergen (Norway), Ruhr-Universität Bochum (Germany) and at the University of Ghent. Regular guest lecturer at University of Piraeus (Greece). European Information Security Award in the area of academic research (2003) Honorary Certified Information Security Manager (CISM) of the Information Systems Audit and Control Association (ISACA) (2003) RSA Award for Excellence in the Field of Mathematics (2014) Member of the Academia Europaea (since 2014). Fellow IACR (2015) IACR Distinguished Lecturer (2016) Christian Beckman award from IFIP TC-11 (2016) ESORICS Research Excellence Award (2017) IT Person of the Year, Belgium (2020) Testimony for the Flemish, Belgian and European Parliament
Memberships	Advisory Board of several start-up companies, research labs and research projects. Permanent Stakeholders group of ENISA (European Network and Information Security Agency) (2012-present) Academia Europaea (2014-present) Belgian Data Protection Authority (knowledge centre) (2019-present) Belgian Privacy Commission (subcommittee national register) (2012-2018) FSE Steering Committee (1993-present) IACR Board member since 1997; vice president (2003-2007); president (2008-2013) LSEC founding member and Chairman of the board (2004-present) Board member of the Belgian Cyber Security Coalition (2015-present)
Reviews	ERC PE6 (Chair 2015/13, Vice Chair 2011, member 2021/2010); EU FET reviews (2012-), EPSRC Review Panel (2006-), FNRS Panel Member (SEN-3, 2008-2013), FWO Panel Member (W&T5, 2014-2019), NWO Panel Member (2007, 2008, 2013), ATTRACT panel member (Luxembourg, 2012-2019), panel member for ANR (FR, 2006), ACI (FR, Panel Chair, 2000-2005). Member of committee/external reviewer for Faculty Appointments at UGhent, DTU, TU Graz, RU Bochum, TU Wien, TU Hamburg.
Citations	
Courses	Google Scholar: 28500 (h-index 82), Scopus: 10950 (h-index 54), Web of Science: 5784 (h-index 38) Cryptography and network security, discrete mathematics, coding theory, digital communications, advanced methods in cryptology, privacy technologies Leuven, January 2022

