Curriculum Vitae Bart Preneel

Full Professor KU Leuven, Dept. Electrical Eng.-ESAT, COSIC

Studies:

1993 - Doctoral Degree in Engineering (summa cum laude), KU Leuven, Belgium
Design and Analysis of Cryptographic Hash functions
1987 - Master of Electrical Engineering (summa cum laude), MSc (burg. ir.), KU Leuven, Belgium
signal processing, digital and analog communications, chip design, control theory
1987 – Economics, program equivalent to BSc in economics that gives access to MSc in economics, KU Leuven, Belgium

Appointments:

Oct. 06 – present Full Professor (FWO) KU Leuven, Dept. of Electrical Eng.-ESAT
Oct. 03 – Oct. 06 Professor (FWO) KU Leuven, Dept. of Electrical Eng.-ESAT
Oct. 03 – Oct. 06 Associate Professor (FWO) KU Leuven, Dept. of Electrical Eng.-ESAT
Sep. 99 – Oct. 03 Assistant Professor KU Leuven, Dept. of Electrical Eng.-ESAT (first year part-time)
Oct. 99 – Oct. 00 Research Associate, FWO, Dept. of Electrical Eng.-ESAT
Oct. 97 – Sep. 00 Part-time Assistant Professor KU Leuven, Dept. of Electrical Eng.-ESAT
Oct. 93 – Oct. 99 Postdoctoral fellow FWO, Dept. of Electrical Eng.-ESAT
Oct. 93 – Oct 94 Visiting Research Fellow, UC Berkeley, Dept. of Electrical Eng.-ESAT
Oct. 99 – Oct. 93 Research Assistant FWO, Dept. of Electrical Eng.-ESAT
Visiting professor positions at University of Ghent (BE), University of Bergen (NO), RU Bochum (DE), TU Graz (AU), DTU (DK). Regular guest lecturer at University of Piraeus (GR). Scientific advisor of Philips Research (2005-2010).

Honors and Awards:

- IT Person of the Year, Belgium (2020)
- ESORICS Outstanding Research Award (2017).
- Kristian Beckman award from IFIP TC11 (2016).
- IACR Distinguished Lecturer in 2016 (the International Association for Cryptographic Research has more than 1600 members and selects one Distinguished lecturer per year).
- IACR Fellow (2015).
- RSA Award for Excellence in the Field of Mathematics (2014).
- Member of the Academia Europaea (since 2014).
- Member of the Expertise Centre of the Belgian Data Protection Authority (since 2019); from 2012-2018 member of the subcommittee national register.
- European Information Security Award for Academic Research (2003).
- Honorary Certified Information Security Manager (CISM) designation by the Information Systems Audit and Control Association (ISACA) (2003).
- Best paper awards at ISC 2008, IEEE International Symposium on Electronic Commerce and Security 2008, Africacrypt 2012.
- Supervisor of Carmela Troncoso, whose PhD thesis has won the ERCIM Security and Trust Management award (2012).
- Supervisor of seven awarded Master Theses.

Scientific expertise:

Discrete mathematics with applications to cryptographic schemes. Design and evaluation of cryptographic algorithms including cryptanalysis, security reductions and proofs. Achievements include the design and analysis of stream ciphers (Trivium), hash functions (RIPEMD-160), block ciphers (SHARK), and authenticated encryption modes (Aegis). Key management and security architectures (including mobile systems, banking, automotive, smart grid). Identity management techniques (identity cards, biometry, secure authentication). Cryptographic protocols for privacy-friendly interactions (electronic voting, insurance pricing, road pricing, proximity tracing). Secure hardware and software implementations including trusted computing, software obfuscation, whitebox cryptography and side channel attacks. Application of cryptographic techniques to images and video. Network security and secure routing for mobile networks. Mobile and IoT security.

My expertise covers both fundamental and applied research: I have managed to make progress in fundamental research and translate this in a period of 5-10 years through various projects into applications that touch a large number of users. I have reviewed and improved many industry standards and specs (those reviews have frequently identified serious security flaws) and I have edited five ISO standards. My work has influenced the Belgian identity card, the Belgian electronic voting scheme, and many widely used standards such as the EMV (Europay-Mastercard-Visa) payment standard. I have testified for the Belgian and European Parliament and I appear regularly in the media to clarify issues related to security and privacy that touch the broader public.

Activities:

(Selected) Chair of program committees: FSE 1994, CMS 1999, Eurocrypt 2000, CT-RSA 2002, SAC 2005, ICALP 2006, ISC 2006, Africacrypt 2009, ESORICS 2010, CHES 2011, APF 2014, FC 2016, Articcrypt 2016, FSE 2017, ACNS 2018, Indocrypt 2021.

(Selected) Program committee memberships: I have served on more than 250 program committees including 61 program committees of IACR conferences and workshops, more than any other researcher. In addition, I have served on 11 program committees of top security conferences. The list includes Crypto (15), Eurocrypt (9), Asiacrypt (10), AMC CCS (10), IEEE Security and Privacy, FSE (19), CHES (4), SAC (8), Indocrypt (8), Africacrypt (4).

(Selected) Editor of Journals: I have served as Editor in Chief of the Transactions on Symmetric Cryptology and as Associate Editor of ACM Transactions on Information Security, Journal of Cryptology, Journal of Computer Security, International Journal of Information & Computer Security, Cryptologia, and IEEE Transactions on Information Forensics and Security. Guest editor for several special issues.

External examiner on 70 PhD or Habilitation committees outside KU Leuven.

(Selected) Member of Scientific Evaluation Committees: ERC PE6 (Chair 2015/13, Vice Chair 2011, Member 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 Delft, TU Graz, RU Bochum, TU Wien, TU Hamburg.

(Selected): Member of Advisory Boards: TCPA (2000-2002), Hypertrust (2000-2007), Intrinsic-ID (2009-), EU SecureIST (2005-2007), EU Riseptis (2007-2009), EU FutureID (2013-), UbiCrypt, RU Bochum, Germany (2013-), CDT Cyber Security, London (2012-), Claude Shannon Institute for Discrete Mathematics, Ireland (2007-2012), CASED, Darmstadt, Germany (2013-2016), CRISP (chair), Darmstadt, Germany (2017-2018), Athena, Darmstadt, Germany (2019-), SBA Research Austria (2013-), ENISA (Permanent) Advisory Group (2012-2022).

Board memberships: chairman of the board of LSEC (organization bringing together 100+ cybersecurity companies) (2004-), Belgian Cyber Security Coalition (2016-), co-founder Nextauth (startup) (2018-), Approach Belgium (2021-).

Invited talks and keynotes: more than 120 in 50 countries including: SAC 1995, FSE 2001, PKC 2002, Wisa 2002, Asiacrypt 2005 and 2010, CARDIS 2006, EuroPKI 2007, Wisec 2009, IFIP SEC 2009, Indocrypt 2010, CT-RSA 2010, Africacrypt 2011, CANS 2012, ICISC 2014, Qcrypt 2014, SACMAT 2015, Eurocrypt 2016, Escar 2018, Esorics 2019, Indocrypt 2019, Chinacrypt 2021.

Graduated Ph.D. students since 2001: 70. 12 have professor positions (9 outside Belgium); seven have taken up research positions in top research labs of Google, IBM, Microsoft, and Philips.

Supervised postdoctoral researchers since 2009: 48 (25% have obtained their Ph.D. outside the KU Leuven).

Publications and citations: more than 100 papers in international journals and more than 400 papers in international conferences with review. Editor of 28 books or proceedings. Inventor of five patents.

- Google scholar: 28500 citations and h-index 82.
- Aminer: more than 22000 citations and h-index 74.
- Scopus: 10950 citations and h-index 54.
- Web of Science: 5784 citations (excluding self-citations) and h-index 38.
- Microsoft Academic Search (2016): 4300 citations (ranked #24 in Security and Privacy Area for last 10 years).
- IACR publications: 80 (ranked #14); IACR service in program committees: 61 (ranked #1); see http://www.iacr.org/cryptodb/data/stats.php.