

KARTHIKEYAN BHARGAVAN

PERSONAL DATA

Date of Birth 7 March, 1976
Nationality India
Languages English, Hindi, Tamil, French
Address 16 rue du Commandeur, Paris 75014, France
Phone +33 6 86 62 76 60
Email karthik.bhargavan@gmail.com
Web <https://karthik.bhargavan.info>

EDUCATION

2012 **H.D.R.**, École normale supérieure, Paris, France
Habilitation à diriger des recherches
Title: Towards the Automated Verification of Cryptographic Protocol Implementations
Graduation Date: May 2012

1997–2003 **Ph.D.**, University of Pennsylvania, Philadelphia, USA
Ph.D. in Computer and Information Science
Supervisor: Carl A. Gunter
Title: Network Event Recognition
Graduation Date: December 2003

1997–1999 **M.S.**, University of Pennsylvania, Philadelphia, USA
Master of Science in Engineering
Graduation Date: August 1999

1993–1997 **B.Tech.**, Indian Institute of Technology, Delhi, India
Bachelor of Technology (Computer Science and Engineering)
Graduation Date: August 1997

EMPLOYMENT

2023–Present *Co-Founder and Chief Research Scientist*, Cryspen, Paris France
A company building high-assurance cryptographic software.
Starting Date: 1 May, 2023

2015–Present *Directeur de recherche*, Inria, Paris France
Research on programming languages and security.
Leader of the PROSECCO research team
Starting Date: 1 January, 2015

2009–2014 *Chargé de recherche contractuel*, Inria, Paris France
Research on programming languages and security.
Starting Date: 1 October, 2009

2004–2009 *Researcher*, Microsoft Research, Cambridge UK
Research on web services security, formal verification, virtualization.
Starting Date: 1 October, 2004

2002–2004 *Post-Doctoral Researcher*, Microsoft Research, Cambridge UK
Research on web services security, network protocol analysis, replication.
Starting Date: 2 December 2002

PERSONAL RESEARCH GRANTS

- 2022–2025** Principal Investigator, DST-Inria Associate Team
Title: VeriSPro: Verifying Security Properties of Group Messaging Protocols
- 2022–2023** Principal Investigator, ERC Proof-Of-Concept Grant 2022
Title: CRYSPEN: Custom Cryptographic Solutions with Formal Security Guarantees
- 2019–2025** Chaire, PRAIRIE Institute Paris
Title: Provably Privacy Preserving Machine Learning
- 2016–2021** Principal Investigator, ERC Consolidator Researcher Grant 2010
Title: CIRCUS: Certified Implementations of Robust, Cryptographically Secure Web Applications
- 2010–2015** Principal Investigator, ERC Starting Independent Researcher Grant 2010
Title: CRYSP: Cryptographically Secure Programs and their Proofs

PRIZES AND AWARDS

- 2019** EU H2020 Horizon Impact Award
- 2017** Distinguished Paper Award at IEEE S&P 2017
- 2016** Prix Jeune Chercheur Inria–Académie des sciences
- 2016** Microsoft Research Outstanding Collaborator Award
- 2017** Distinguished Paper Award at NDSS 2016
- 2016** Levchin Prize for Real World Cryptography
- 2015** Distinguished Paper Award at ACM CCS 2015
- 2015** Distinguished Paper Award at IEEE S&P 2015
- 2015** Distinguished Paper Award at WOOT 2015
- 2015** Pwnie Award at BlackHat 2015
- 2003** The Morris and Dorothy Rubinoff Dissertation Award

PHD STUDENTS

- Current** Son Ho, Théophile Wallez
- Graduated** Evmorfia-Iro Bartzia, Antoine Delignat-Lavaud, Jean Karim Zinzondohoué, Benjamin Beurdouche, Marina Polubelova, Natalia Kulatova, Denis Merigoux, Benjamin Lipp

SELECTED COMMITTEES

- 2020–** ACM TOPS Journal (Associated Editor)
- 2017–** HACS Workshop (Organizing Committee Member)
- 2020–** VeriCrypt Workshop (co-chair)
- 2021** IndoCrypt 2021 (co-chair)
- 2006–2023** IEEE Security & Privacy (S&P 2016-2022)
ACM Conference on Computer and Communications Security (CCS 2015-2022)
IEEE Computer Security Foundations (CSF 2016-2022)
Principles of Programming Languages (POPL 2015, 2023)
Applied Cryptography and Network Security (ACNS 2020)
Real World Cryptography Conference (RWC 2020)
World Wide Web Conference (WWW 2017)
Principles of Security and Trust (POST 2015)
Workshop on Programming Languages and Analysis for Security (PLAS 2013)
Symposium On Applied Computing (Security 2015, Software Verification 2008)
International Conference on Computer-Aided Verification (CAV 2006)