

# Curriculum Vitae - Lars R. Knudsen

## Profile

- Ridder af Dannebrog, August 2021. Knight of the Dannebrog
- Google scholar: 15168 Citations, h-index 45. (20.04.2023)
- Full professor 1999-2022, published 11 books and more than 120 scientific articles.
- Head of the Cryptology and Cyber Security Group at the Technical University of Denmark 2001-2018.
- Academy of Technical Sciences, Denmark, member since 2005.
- Co-founder and chief cryptologist at Dencrypt A/S
- Co-founder and chief cryptologist at PiiGuard ApS
- Two patents, one pending.



## Education

- PhD, Computer Science, Aarhus University, Denmark, 1994
- MSc, Computer Science and Mathematics, Aarhus University, Denmark, 1992
- Advanced commercial school, 1982-1984
- Bank assistant and clerk (incl. banking school), 1979-82

## Employment

- Professor University of South Denmark, April 2023-
- Senior Executive Consultant, Danish Defense, Feb 1, 2022 - March 31 2023
- Adjunct professor, Aalborg University, Denmark, from Sept. 1, 2022
- Professor, Technical University of Denmark, Kgs. Lyngby, from Sept 2001-2022
- Leave from DTU to work in Dencrypt A/S, Sept. 2018 – Aug. 2019.
- Adjoint professor, University of Bergen, Norway, Jan 2002 - Dec 2007
- Professor, University of Bergen, Norway, Apr 1999 - Sept 2001
- Associate Professor, University of Bergen, Norway, Jan 1998 - Apr 1999
- Lecturer, University of Bergen, Norway, Sept 1997 - Jan 1998
- Postdoctoral Researcher, Katholieke Universiteit, Leuven, Belgium, Feb 1996 - Sept 1997
- Postdoctoral Researcher, The Danish Technical Science Foundation, Feb 1995 - Feb 1996
- Research Assistant, Lecturer, Aarhus University, Denmark, Aug 1994 - Feb 1995
- Research Associate, Aarhus University, Denmark, Feb 1992 - Aug 1994
- Employed in a Danish bank, 1979-1982

## Research Interests

- Main interest is cryptography and the published work is in the areas of secret key algorithms,

cryptographic hash functions, message authentication codes, micro payment systems, identification schemes, key escrow systems and postquantum cryptology.

## Teaching experiece

The first time I taught at university level was in the autumn semester 1994 at Aarhus University. In the fall of 1997 I joined University of Bergen as an assistant professor and I have been teaching almost every semester since then until the end of 2021. I have taught many levels of cryptology over the years, but also courses in coding theory and discrete mathematics.

## Representation

- Fellow of IACR (International Association of Cryptology Research), from 2013. [www.iacr.org](http://www.iacr.org)
- Member of ATV, the Danish Academy of Technical Sciences, Denmark, from 2005 (by invitation only). Member of the steering committee in the Electro and IT group 2013-2017.
- Member of Virksomhedsrådet for IT-sikkerhed under Erhvervsministeriet, 2018-2020.
- Chairman of the Selection Committee for “Cyber Security Prize” appointed by DANISH IT's Councils for information security, 2016.
- Member of “Rådet for digital sikkerhed”, the Council for Digital Security Denmark, 2013-17
- Head of the section Cyber Security at the Department of Applied Mathematics and Informatics, Technical University of Denmark, Jan 2015-Aug. 2018.
- Head of the section Cryptology at the Department of Applied Mathematics and Informatics, Technical University of Denmark, 2013-2015.
- Center manager of the research centre "Center for Information Security" at DTU, involving four different departments, 2014-2016.
- Head of the Discrete Mathematics group at the Department of Mathematics, Technical University of Denmark, 2006-2012.
- Head of Department, Department of Mathematics, Technical University of Denmark, 2009.
- Deputy Head of Department, Department of Mathematics, Technical University of Denmark, 2006-2009.
- Elected director of IACR, International Association of Cryptologic Research for the periods of Jan 2001-Dec 2003 and Jan 2004-Dec 2006, <http://www.iacr.org>.
- Chairman of the steering committee of the conference series Fast Software Encryption, sponsored by the IACR, 2007-2010, regular member 1998-2007.
- General chair of the IACR conference Eurocrypt, Copenhagen, Denmark, May 2014, 350 participants.
- General chair of the IACR workshop Fast Software Encryption held at the Technical University of Denmark, February 2011, 150 participants.
- Organiser of the workshop SKEW held in Århus, May 2005, 102 participants.

## Projects and grants

- Research project ” Quantum Safe Cryptography” joint with Dencrypt A/S (Inc.). Grant from Medfinansieringsfonden (Danish Defense) for 7.8 million DKK, 2019.
- Research project ”Post-Quantum Secure Symmetric Cryptography”, from Danmarks Frie Forskningsfond, Teknologi og Produktion, (joint with Andrey Bogdanov), 2.6 million DKK, 2018.

Manager of the participation of the Technical University of Denmark in PQCrypto, a network of excellence supported under the Horizon 2020 framework of the European Commission, H2020-ICT-2014-1, 2015-2018.

- Organiser of summer school in cryptology in Reykjavik, Iceland, June 6-12, 2013. Received grants for a total of DKK 350,000 for this event.
- Organiser of summer school in cryptology in Sardinia, Italy, October 19-22, 2015.
- Organiser of summer school in cryptology in Malaga, Spain, February 19-23, 2018.
- Manager of the research project Lightweight Cryptology sponsored by the Danish Research Council for Technology and Innovation, 2013-2016, 2.7 million DKK.
- IBM Faculty Award 2013 to support to establish Master's degree in Cyber Security at Technical University of Denmark.
- Guest professorship grant for a 3-month visit of Professor Anne Canteaut, INRIA, France 2012. The Otto Mønsted Foundation.
- Personal grant for a 6-months sabbatical from The Danish Council for Independent Research, Natural Sciences, 200,000 DKK, 2009.
- Postdoctoral grant (2 years) for Praveen Gauravaram from the Danish Research Council for Technology and Innovation, 1.6 million DKK, 2009.
- Manager of the participation of the Technical University of Denmark in ECRYPT II, a network of excellence supported under the 7th framework of the European Commission, 2008-2012.
- Manager of the research project New Cryptology sponsored by the Villum Kann Rasmussen Foundation, 2008-2011, 4.2 million DKK.
- Manager of the research project Cryptanalysis of Symmetric Cryptographic Algorithms by means of Numerical Methods sponsored by Danish Agency for Science, Technology and Innovation, 2008-2011, 2.5 million DKK.
- IT-security prize 2010 in Germany for the design of the lightweight block cipher PRESENT.
- Co-organiser of the workshop Hash Functions in Cryptology: Theory and Practice held at the Lorentz Center, Leiden, The Netherlands, June 2-6, 2008.
- Postdoctoral grant for Praveen Gauravaram from the Danish Research Council for Technology and Innovation, DKK 770,000, 2008.
- Guest professorship grant for a 3-month visit of Professor Bart Preneel, K.U Leuven, Belgium, 2007. The Otto Mønsted Foundation.
- Grant from DCSC, Danish Centre for Scientific Computing, CPU-0107-03: Cryptanalysis of Symmetric Cryptographic Algorithms, 2007, DKK 250,000. (Purchase of SUN super-computer).
- Guest professorship grant for a 3-month visit of Professor Vincent Rijmen, K.U Leuven, Belgium, 2006. The Otto Mønsted Foundation.
- Manager of the research project Digital signatures, sponsored by Danish Agency for Science, Technology and Innovation, 2005-2008, 3 million DKK.
- Manager of the participation of the Technical University of Denmark in ECRYPT, a network of excellence supported under the 6th framework of the European Commission, 2004-2008, see <http://www.ecrypt.eu.org>, EU 87,000.
- Co-manager of the centre Foundations in Cryptology and Security (FICS), 2002-2006, supported by the Danish National Council of Research, 6 million DKK.
- Partner manager in NESSIE (New European Schemes for Signatures, Integrity, and Encryption), a project within the Information Societies Technology (IST) Program of the European Commission (Key Action II, Action Line II.4.1), EU 260,000.

### Postdoctoral students

- Samir Hodzic, 2019-2021.
- Ashutosh Dhar Dwivedi, 2020-2021.

- Qingju Wang (2016-2018)
- Stefan Kølbl (2016-2018)
- Tyge Tiessen (2016-2017)
- Subhadeep Banik (2014)
- Mohamed Ahmed Abdelraheem (2014)
- Martin Albrecht, 2013
- Christina Boura, 2012-2013
- Christiane Peters, 2011-2013
- Julia Borghoff, 2011-2013
- Krystian Matusiewicz, 2008-2010
- Praveen Gauravaram, 2007-2011

### **PhD student supervision (year finished in brackets)**

- Freja Elbro, 2020-
- Tommaso Ricci, 2020-2022.
- Andreas Brasen Kidmose (2022).
- Tyge Tiessen (2016)
- Stefan Kølbl (2016)
- Martin M. Lauridsen (2015)
- Hoda Alkhzaim (2015)
- Mohamed Ahmed Abdelraheem (2013)
- Julia Borghoff (2011)
- Valerie Gauthier Umana (2011)
- Charlotte Vikkelsø Miolane (2009)
- Søren S. Thomsen (2009)
- John Erik Mathiassen (2005)
- Håvard Raddum (2004)

### **Editorial experience**

- Associate editor of Design, Codes and Cryptography (2011-2019).
- Associate editor of IEEE Transactions on Information Forensics and Security (2010-2012).
- Associate editor of the Journal of Cryptology (2003-2010).
- Associate editor of IET Information Security (2006-2007).

### **Organisational experience**


- Program chair of the conference BalkanCryptSec, Slovenia, September 2015.
- Program chair of the conference Selected Areas in Cryptography (SAC 2012), Windsor, Canada, August 2012.
- Program chair of the conference Eurocrypt 2002, Amsterdam, May 2002.
- Program chair of the conference Fast Software Encryption 6, Rome, Italy, March 1999

### **Courses on management and other**

- Mini-MBA, 6 months, Nov 2012-May 2013. Probana Business School, Copenhagen.
- Mindfulness, 1 day, 2011. DTU.

- Interview techniques, 1 day, 2009. DTU.
- The optimal research application, 1 day, 2007. DTU.
- Coaching, 1 day, 2007. DTU.
- Performance appraisal, 1 day, 2006. DTU.
- Intercultural competences, 2 days, 2005. Magisterforeningen.
- DTU Manager Course, 4 days, 2005. DTU.

### **Business**

- Co-founder, Board Member and Chief Cryptologist of Dencrypt A/S (Ltd), December 2013.
- Co-founder and Chief Cryptologist of PiiGuard ApS, July 2018.
- Consulting company ABT ApS from 2004 to 2021, together with Professor Bart Preneel, Belgium. 

### **Personal data**

- Born on February 21st 1962 in Skrydstrup, Denmark
- Three children, born 1997, 1999, 2003.
- Languages: Danish (fluent), English (fluent), German (good), Dutch (fair), Spanish (beginner).
- Blog <https://larsknudsen.wordpress.com/>

### **Contact info**

- Else Alfeltsvej 74C, 4th, DK-2300 København S., +45 5180 1510, [lars@ramkildeknudsen.dk](mailto:lars@ramkildeknudsen.dk)

### **Sports and Hobbies**

I have won numerous local and regional championships in ice hockey and in football (soccer) in Denmark, and I was the Danish Champion in ice hockey 1977-78. I have a big passion for music and play the guitar. I have played in three different (amateur) pop/rock bands, twice as leader/organiser. I have played chess from the age of five, though in later years I have not participated in tournaments.