

CURRICULUM VITAE FOR TOR E. BJØRSTAD

PERSONAL INFORMATION:

Full Name: Tor Erling Bjørstad
Address: Skivebakken 20A, N-5018 Bergen, Norway
Telephone: (+ 47) 97 08 77 22 (mobile)
E-mail: tor.bjorstad@ii.uib.no (work)
torebj@gmail.com (private)
Home page: <http://www.ii.uib.no/~tor/>
LinkedIn: <http://www.linkedin.com/in/torbjorstad>
Date of birth: March 12th, 1982
Place of birth: Oslo, Norway

EDUCATION:

2006 - present University of Bergen, Norway. PhD in Cryptography.
Thesis: "On the Security of Cryptographic Primitives" submitted Dec. 2009.
Advisor: Associate professor Matthew Parker.
2009 Katholieke Universiteit Leuven, Belgium. Visiting Scholar, January - May.
2000 - 2005 Norwegian University of Science and Technology.
Master's Degree in Applied Physics and Mathematics.
Advisor: Professor Alexei Roudakov.
Thesis: "Provable Security of Signcryption".
1998 - 2000 International Baccalaureate at Bergen Cathedral School, Norway.
Bilingual diploma awarded.

PEER-REVIEWED PUBLICATIONS:

1. T. E. Bjørstad and A. W. Dent.
Building Better Signcryption Schemes with Tag-KEMs.
Proc. PKC 2006. Springer-Verlag LNCS vol. 3958, pp. 491-507.
2. T. E. Bjørstad, A. W. Dent and N. P. Smart.
Efficient KEMs with Partial Message Recovery.
Proc. 11th IMA Conf. on Cryptography and Coding, Springer-Verlag LNCS vol. 4887, pp. 233-256.
3. E. Käsper, V. Rijmen, T. E. Bjørstad, C. Rechberger, M. Robshaw and G. Sekar.
Correlated Keystreams in Moustique.
Proc. AFRICACRYPT 2008, Springer-Verlag LNCS vol. 5023, pp. 246-257.
4. T. E. Bjørstad.
Cryptanalysis of Grain using Time / Memory / Data Tradeoffs.
Pre-proceedings of International Workshop of Coding and Cryptography (WCC) 2009.
Submitted to Journal of Designs, Codes and Cryptography.

OTHER PUBLICATIONS:

1. T. E. Bjørstad and M. G. Parker
Equivalence Between Certain Complementary Pairs of Types I and III.
Post-proceedings of NATO Advanced Research Workshop, Bulgaria, 2008.
2. O. Dunkelman and T. E. Bjørstad
Practical Attacks on NESHA-256
Cryptology ePrint Archive, Report 2009/384.

WORK EXPERIENCE:

- 2006 - present University of Bergen, Norway. Research fellow, Dept. of Informatics.
Junior researcher, with 25% teaching duties at the department.
- 2004 - 2005 NTNU, Trondheim, Norway. Teaching assistant, Dept. of Mathematical Sciences.
- 2004 Det Norske Veritas, Høvik, Norway. Summer intern, DNV Software.
Design and implementation of meshing software in C++.
- 2002 Det Norske Veritas, Høvik, Norway. Summer intern, DNV Software.
Modelling and structural analysis of container ship hulls.
- 2001 Schenker BTL, Oslo, Norway. Summer intern, Service Department.

OTHER ACTIVITIES:

- 2007 - present Bergen municipal court. Lay judge (“meddommer”).
- 2007 - 2009 Electoral Commission, Young Liberals of Norway.
Member (2007-2008) / leader (2008-2009).
- 2006 - 2008 National council, Young Liberals of Norway. Member.
(2006-2007 by direct appointment, 2007-2008 representing the Hordaland region.)
- 2007 The oversight committee (“kontrollutvalget”), City of Bergen. Deputy member.
- 2001 - 2002 Cybercamp, Trondheim, Norway. Volunteer.
- 2000 - 2001 UKA 2001, Trondheim, Norway. Volunteer.
Computer networks and application development for large student festival.
- 2000 European Space Camp. Participant.
- 1999 - 2000 Norwegian Mathematics Olympiad (IMO qualifier). National finalist (twice).

LANGUAGES:

- Norwegian: Native speaker.
- English: Fluent.
- German: Basic.