Dr. Alexander Dent

Information Security Group, Royal Holloway, University of London
http://www.cogentcryptography.com/
adent@qti.qualcomm.com

Summary

- Security engineer for a leading telecommunications company with involvement in a large number of security review and design projects.
- World-class researcher in security algorithms and protocols, with over thirty research papers published in top-level international peer reviewed security conferences, books, and journals (including Eurocrypt, Asiacrypt, and the Journal of Cryptology).
- Extensive experience in the design and evaluation of security algorithms and protocols from practical and commercial viewpoints, including eight years experience as a UK expert on the ISO/IEC standardisation committee and two years experience on the EU's NESSIE algorithm evaluation project.
- Eight years experience in teaching a wide range of information security techniques to a post-graduate class with differing levels of experience and technical backgrounds.
- Practical syllabus development experience in the design of both the campus-based and online information security courses and a course in complexity theory with applications to communication systems.

Employment & Achievements

July 2011 to date **Staff Engineer (Qualcomm)**

- Manager for small team of security engineers.
- Responsibility for securing commercial Qualcomm products.
- Team lead for threat modelling training activities throughout Qualcomm.
- Team lead for security activities involving the Bluetooth, WiFi and NFC.

Nov 2009 to June 2011 **Reader (Royal Holloway, University of London).**

- Position equivalent to Associate Professor.
- Extensive research on public-key algorithms and protocols.
- Co-editor of a research-level textbook on signcryption technologies.
- Significant research on organisational information security management systems.
- Supervisor of two doctoral student theses in theoretical and practical cryptography.
- Supervisor of over a thirty M.Sc. students' theses covering all aspects of information security.
- Served as a UK expert on the ISO/IEC SC27/WG2 standardisation committee working on the standardisation of practical cryptographic algorithms and protocols (from 2001).

Jan 2006 to June 2011 **Commercial Consultant**

- Technical consultant to Lloyds Register Quality Assurance (LRQA) on PKI compliance issues, including an assignment for a major UK government customer.
- Employed as a security consultant by the Opencoin e-cash project to evaluate the cryptographic algorithms and infrastructures useable in an electronic cash system.

Jan 2006 – Nov 2009 **Lecturer (Royal Holloway, University of London)**

- Position equivalent to Assistant Professor.

Jan 2004 – Dec 2005 **Junior Research Fellow (Royal Holloway, University of London)**

- Successfully bid for funding in the prestigious EPSRC Junior Research Fellowship program.
- Co-author of a post-graduate-level textbook on standardised information security techniques.

Jan 2003 – Dec 2003 **Temporary Lecturer (Royal Holloway, University of London)**

- Managed a group of doctoral and post-doctoral researchers for the Mobile VCE industrial consortium.

Sep 2001 – Dec 2002 **Research Assistant (Royal Holloway, University of London)**

- Significant research and analysis contributions to the EU's cryptographic algorithm evaluation project NESSIE, with particular reference to public-key algorithms and protocols.

EDUCATION

Oct 1998 – Sep 2001 **Ph.D. degree (Royal Holloway, University of London)**

- Thesis on combinatorial design theory, entitled "On the theory of point-weight designs".
- EPSRC funded studentship with CASE award from RACAL.

Sep 1994 – Jul 1998 **M.Math degree (St. Peter's College, University of Oxford)**

- First class honours achieved in both bachelor's and master's exams.
- Prizes: St. Peter's College exhibition award (1995); St. Peter's College scholarship award (1997); Charles Caine Mathematics Prize (1998).

RESEARCH INTERESTS

- **Complexity Theory of Mathematical Cryptography**. Extensive and in-depth knowledge of the theory of mathematical cryptography and particularly the provable security paradigm.
- **Development of Public-Key Cryptography Algorithms and Protocols**. Extensive research in the development of secure and practical public-key algorithms and protocols.
- **Formal Theory of Information Security Management**. A research interest in the burgeoning field of formal analysis within information security management systems.
- **Combinatorial Design Theory**. A minor research interest in mathematical design theory and related combinatorial problems.

PROFESSIONAL ESTEEM INDICATORS

- Awarded a prestigious EPSRC Junior Research Fellowship Award.
- Member of the ITA research project (jointly funded by the US Department of Defense and the UK Ministry of Defence) and successfully bid for $280k in research funding.
- Internal Ph.D. examiner for the doctoral student Jihoon Cho.
- External examiner for the Information Security course at Gjøvik University College, Norway.
- Co-editor of the original ISO/IEC 18031 international standard on random bit generation.
- Co-author of the proposal to standardise the SK-KEM identity-based encryption scheme by the IEEE 1363 standardisation body. This proposal has been accepted for inclusion in the standard.
- Co-holder of the patent "A method for the provision of device time/location information". U.K. patent number GB0502919.4 and U.S. patent number 7,698,554.
- Invited speaker at the ECRYPT Provable Security Workshop in 2005 and ECRYPT II Provable Security Summer School in 2009.
- Invited speaker at the Africacrypt 2008, EuroPKI 2009, ProvSec 2009 conferences.
- Programme committee member for CT-RSA 2004; ICISC 2004; CT-RSA 2007; CANS 2007; ACNS 2008; CT-RSA 2009; WIFS 2009; Africacrypt 2010; ProvSec 2010; CT-RSA 2010; PKC 2011; EuroPKI 2011; CT-RSA 2012.

REFERENCES

References available on request