Presentations, seminars and tutorials

1. 10 August 2011, at 2:30pm. *Manual authentication protocols*. Presented at the Naval Postgraduate School, Computer Science Department, Monterey, California, USA. Host: Professors Berzins Valdis and Luqi.

2. 2 August 2011, at 11:00am. *Rational authentication* protocols. Presented at the Naval Research Laboratory, the Center for High Assurance Computer Systems, Washington DC, USA. Host: Drs Catherine Meadows and Paul Syverson.

3. 29 July 2011, at 11:00am. *Rational authentication* protocols. Presented at the IBM T.J. Watson Research Center, the Cryptography Research Group, Hawthorne, New York, USA. Host: Drs Tal Rabin, Shai Halevi and Rosario Gennaro.

4. 27 July 2011, at 1:00pm. *Rational authentication protocols*. Presented at the Palo Alto Research Center or Xerox PARC, the Security and Privacy research group, Palo Alto, California, USA. Host: Dr. Richard Chow.

5. 25 May 2011, at 11:30am. *Rational authentication protocols.* Presented at the Concurrency, Verification and Security Seminar Series at the Oxford University Department of Computer Science, UK. Host: Mr. Philip Amrstrong. URL Link: http://www.cs.ox.ac.uk/seminars/587.html

6. 7 April 2011, at 5:20pm. *Rational authentication protocols.* Host: Dr. Tom Chothia. Presented at the Fifth CryptoForma meeting at the University of Birmingham, UK. Link: http://www.cryptoforma.org.uk/meet5.html

7. 9 March 2011, at 11:30am. O*n the cryptography of digest functions in manual authentication protocols*. Presented at the Concurrency, Verification & Security Seminars, Oxford University Computing Laboratory, Oxford, UK. Host: Mr. Philip Armstrong. URL Link: https://www.comlab.ox.ac.uk/seminars/567.html

8. 21 February 2011, at 2:00pm. *Rational authentication protocols.* Host: Dr. Atefeh Mashatan. Presented at LASEC meeting, ECOLE POLYTECHNIQUE FEDERALE DE LAUSANNE, LASEC-Security and Cryptography Laboratory. Lausanne, Switzerland.

9. 8 February 2011, at 3:00pm. *On the cryptography of universal hash functions in manual authentication protocols*. Host: Professor Serge Vaudenay. Presented at ECOLE POLYTECHNIQUE FEDERALE DE LAUSANNE LASEC-Security and Cryptography Laboratory. Lausanne, Switzerland. Link: http://lasecwww.epfl.ch/php_code/seminars/display_details.php?id=69

10. 28 September 2010, at 2:30pm. *On the cryptography of universal hash functions in manual authentication protocols*. Host: Dr. Frederik Vercauteren.

Katholieke Universiteit Leuven, Computer Security and Industrial Cryptography group, Leuven, Belgium.

11. 9 November 2009. *Authentication protocols based on human interaction in security pervasive computing*. Host: Professor Gene Tsudik. University of California, Irvine, Security and Privacy Research OUTfit group, California, USA.

12. 7 September 2009. *New combinatorial bounds for almost universal hash functions*. The Summer School on Provable Security, a short presentation, Barcelona, Spain. (Link: http://www.cs.bris.ac.uk/Research/CryptographySecurity/SummerSchool2009/programme.html)

13. 3 June 2009. *Authentication protocols based on human interactions in pervasive computing*. Host: Dr. Eerke Boiten. The first official meeting of CryptoForma, Royal Holloway, University of London. Link: http://www.cryptoforma.org.uk/meet1.html

14. 14 May 2009, at 3pm. *Authentication protocols based on human interaction in security pervasive computing*. Host: Professor Andrew Chi-Chih Yao. Tsinghua University, Institute of Theoretical Computer Science seminar series, Beijing, China.

15. 12 May 2009. *Authentication protocols based on human interaction in security pervasive computing*. Host: Dr. Xie Shuling. East China Normal University, Software Engineering Institute. Shanghai, China

16. 11 May 2009. *Authentication protocols based on human interaction in security pervasive computing.* Host: Professor Kefei Chen. Shanghai Jiao Tong University, Cryptography and Security group, China.

17. 24 April 2009. *Application of universal hashes in authentication protocols based on human interaction in pervasive computing*. Host: Professor Yvo G. Desmedt. University College London, Information Security group, UK. Link: http://www.cs.ucl.ac.uk/teaching/mscisec/InformationSecuritySeminars.htm

18. 1st July 2008, at 11am. *Separating two roles of hashing in one-way message authentication.* Host: Dr. Diana Smetters. The security group of the PaloAlto Research Center (PARC, Xerox Lab), Palo Alto (California), USA. (Link: http://www.parc.com/research/projects/security/default.html).

19. 30th June 2008, at 3pm. *Separating two roles of hashing in one-way message authentication.* Host: Professor John Mitchell. Presented at the Stanford University, Palo Alto (California), USA. (Link: http://crypto.stanford.edu/seclab/).

20. 24th June 2008, at 12pm. *Separating two roles of hashing in one-way message authentication.* Host: Professor Adrian Perrig. Presented at the CyLab of the Carnegie Mellon University, Pittsburgh (Pennsylvania), USA. (Link of

abstract: http://www.cylab.cmu.edu/default.aspx?id=2467). The same talk was also given at the workshop of FCS-ARSPA-WITS'08 at 2pm on 20th June 2008, also organised at CMU.

21. 25th January 2008, at 2pm. *Authentication protocols based on human interaction in security pervasive computing.* Host: Professor Kaisa Nyberg. Presented at *the Helsinki University of Technology, Finland,* Laboratory of Theoretical Computer Science Abstract .

22. 21st January 2008, at 2pm. *Authentication protocols based on human interaction in security pervasive computing.* Host: Drs Baptiste Alcalde and Sasa Radomirovic. Presented at *the University of Luxembourg, Luxembourg,* Laboratory of Algorithmics, Cryptology and Security Abstract .

23. 18th January 2008, at 2pm. *Authentication protocols based on human interaction in security pervasive computing.* Host: Dr. Jaap-Henk Hoepman. Presented at *the Radboud University Nijmegen, The Netherlands,* the Institute for Computing and Information Sciences, the Security of System Group Abstract .

24. 17th January 2008. *Application of Universal Hash functions in authentication protocols based on human interaction in security pervasive computing.* Host; Professor Bart Preneel. Presented at *Katholieke Universiteit Leuven, Belgium,* Electrical Engineering Department, Computer Security and Industrial Cryptography group (COSIC) .

25. 11th December 2007. *Authentication protocols based on human interaction in security pervasive computing.* Host: Professor Dr. Srdjan capkun. Presented at *ETH Zurich: Eldgenossische Technische Hochschule Zurich* (Swiss Federal Institute of Technology Zurich), Department of Computer Science System Security Group . Zurich, Switzerland.

26. 10th December 2007, at 2pm. *Authentication protocols based on human interaction in security pervasive computing.* Host: Professor Serge Vaudenay. Presented at *ECOLE POLYTECHNIQUE FEDERALE DE LAUSANNE* LASEC-Security and Cryptography Laboratory . Lausanne, Switzerland.

27. 14th November 2007, at 11.30am. *Authentication protocols based on human interaction. Concurrency & Security Seminars at Oxford University Computing Laboratory.* Abstract .

28. 13th November 2007, at 4.15pm. *Authentication protocols based on human interaction in security pervasive computing.* Host: Professor Ross Anderson. Presented at *The Security Seminar Series, Computer Laboratory Security Group, University of Cambridge* Abstract .

29. 6th November 2007, at 2pm. *Authentication protocols based on human comparison of short digests in security pervasive computing.* Host: Professor Nigel Paul Smart. Presented at *The Enigma Variations : The Bristol University Information Security Seminars* Abstract .

30. 11th October 2007, at 4pm. *Authentication protocols based on human interaction in security pervasive computing.* Host: Professors Kenny Paterson and Chris Mitchell. Presented at *The Royal Holloway Information Security Seminars, University of London* Abstract .

31. 10th October 2007, at 2pm. *Authentication protocols based on human interaction in security pervasive computing.* Host: Dr. Siraj Shaikh. Presented at the *Department of Information Systems, Cranfield University, Defense Academy of United Kingdom* . Shrivenham, Swindon, UK. Abstract .

32. 13th September 2007. *Authentication protocols based on human comparison of short digests in security pervasive computing.* Host; Dr. Alessandro Aldini. Presented at the *International School on Foundation of Security Analysis and Design* (FOSAD 2007), University Residential Center of Bertinoro, Italy, 9th-15th September 2007. Abstract and Slides .

33. 4th April 2007. *Security in Pervasive Computing: An analytical survey of authentication protocols based on human interaction. The 23rd British Colloquium for Theoretical Computer Science* (BCTCS 07) at St. Anne's College, Oxford University. Abstract and Slides .

34. 17th November 2006. *Authenticating ad hoc network by comparison of short digests. Concurrency & Security Seminars at Oxford University Computing Laboratory.* Abstract .

35. 13th October 2006. *Efficient group authentication protocols based on human interaction. Proceedings of Programming Research Group Conference at Oxford University Computing Laboratory.* Page 5-6. PDF . Slides(PDF) .

36. 12th September 2005. *Compression Algorithm.* Host: Mr Mark Leverington (the manager). Presented at ARM Cambridge, Blackburn (England) . (pdf) Summer internship (after BSc Bristol, and before D.Phil Oxford).