

LONG HOANG NGUYEN

Email: Long.Nguyen@comlab.ox.ac.uk

Date of birth: 23.09.1983

Nationality: Vietnamese

EDUCATION

- 2005-2008** University of Oxford, University College. D.Phil in Computer Science.
Thesis title: Authentication protocols in pervasive security computing (I intend to submit in Aug 2008).
- 2002-2005** University of Bristol. BSc Computer Science. 1st class (84% on average).
- 2001-2002** Bellerbys College. A Level Maths (A, 96%), Further Maths (A, 96%), and Physics (A, 92%).

INTERNATIONAL PATENT AND STANDARD APPLICATIONS

- A.W. Roscoe, L.H. Nguyen. **Security in computing networks**. Published by the *World Intellectual Property Organization (WIPO)*. Publication Number: WO/2007/052045. Publication date: 10.05.2007.
- A.W. Roscoe, B. Chen, L.H. Nguyen. **Improvements in communications security**. International Patent Application No. PCT/GB07/004963.
- L.H. Nguyen, A.W. Roscoe. **Revised version of the international standard ISO/IEC 9798-6**. Submitted to the relevant ISO/IEC UK committee.

PUBLICATIONS

- L.H. Nguyen, A.W. Roscoe. **Authenticating ad-hoc networks by comparison of short digests**. In *Journal of Information and Computation*, Nov 2007.
- L.H. Nguyen, A.W. Roscoe. **Efficient group authentication protocols based on human interaction**. Proc of *Foundation of Computer Security and Automated Reasoning for Security Protocol Analysis* workshop, Aug 2006
- L.H. Nguyen, A.W. Roscoe. **Authentication protocols based on low-bandwidth unspoofable channels: a comparative survey**. Submitted to *Journal of Computer Security*.

PAPERS IN PREPARATION (manuscripts are available)

- L.H. Nguyen, A.W. Roscoe. **New theoretical bounds for universal hash functions**.
- L.H. Nguyen, A.W. Roscoe. **Efficient digest functions based on Toeplitz matrix and integer multiplication**.
- L.H. Nguyen, A.W. Roscoe. **Empirically authenticated one directional message transmission**.

INVITED PRESENTATIONS

- **Security in Pervasive Computing: A survey of authentication protocols based on human interaction**
 - *Helsinki University of Technology and Nokia Research Centre*, Helsinki, Finland, 25th Jan 2008.
 - *University of Luxembourg*, Laboratory of Algorithm, Cryptology and Security, 21st Jan 2008.
 - *Radbound University Nijmegen*, The Netherlands, Security of System Group, 18th Jan 2008.
 - *ETH Zurich*, Switzerland, System Security Group, 11th Dec 2007.
 - *Oxford University*, Concurrency and Security Seminars, 14th Nov 2007.
 - *Cambridge University*, Computer Laboratory Security Group, 13th Nov 2007.
 - *University of London*, the Royal Holloway Information Security Seminars, 11th Oct 2007.
 - The 23rd *British Colloquium for Theoretical Computer Science (BCTCS)*, Oxford, 2nd-5th Apr 2007.
 - The *International School on Foundation of Security Analysis and Design*, Bologna, Italy, 9th-15th Sep 07.
- **Application of universal hash functions in authentication protocols based on human interaction**
 - *Katholieke Universiteit Leuven*, Belgium, Security and Cryptography group, 17th Jan 2008.
- **Authentication protocols based on human interaction in pervasive computing**
 - *Ecole Polytechnique Federale de Lausanne*, Switzerland, LASEC-Crypto Laboratory, 10th Dec 2007.
 - *Bristol University*, the Enigma Variations: the Information Security Seminars, 6th Nov 2007.
 - *Cranfield University*, Defence Academy of United Kingdom, 10th Oct 2007.

AWARDS AND SCHOLARSHIPS

- 2007-2008** G.A. Paul Memorial Scholar: rewarding research excellence, University College, Oxford University.
- 2005-2008** Oxford University Computing Laboratory and Vietnamese government D.Phil scholarships.
- 2005-2008** Overseas research scholarship (ORS), declined.
- July-05** Awards for the best final year computer science undergraduate and project at Bristol University.
- July-04** Award for the best penultimate year computer science undergraduate at Bristol University.
- Summer 04** *Nuffield Science Bursaries* for an undergraduate research project.

TEACHING

- 2006-2008** Teaching tutorials and classes for 5 subjects including Computer Security at Oxford University.