Bingsheng Zhang, Ph.D.

State University of New York at Buffalo
Computer Science and Engineering
340 Davis Hall
Buffalo, New York 14260-2000
Email: bzhang26@buffalo.edu

PROFILE

An intelligent, well-presented and hard-working PhD graduates, with solid qualifications and a comprehensive skill-set. As a researcher who is obsessed with mathematics, computer science and electronic engineering, Mr. Zhang put focus on information security and cryptography, especially on secure two-party/multi-party computation. He also has rich project experiences in risk management, network security and privacy preserving data mining aspects. Mr. Zhang has strong independent R&D capability and feels confidence in both academic research and practical implementation.

EDUCATION

2009 – 2011:	University of Tartu (UT)	(PhD)	Estonia
2007 – 2008:	University College London (UCL)	(Master)	UK
2003 – 2007:	Zhejiang University of Technology	(Bachelor)	China

QUALIFICATIONS AND CERTIFICATIONS

- PhD in Computer Science 2011
- Msc in Information Security 2008
- B.eng in Computer Science and Technology 2007
- B.L in Law (Second Degree) 2007
- Certification for Outstanding Graduate of Zhejiang Province 2007
- Two Qualifications Certificate for Computer and Software Technology Proficiency (In 2006, participants 75,654, passing rate 16.1%, recognized by China, Japan and Korea) Software Engineer and Network Engineer, Intermediate Level 2006
- Excellent Student Second Class and First Class University Scholarships For consecutive three years
- Second Prize in the 4th NEC Cup ACM Collegiate Programming Contest 2006
- Most Distinguished Student Award 2006

WORK EXPERIENCE AND OLD RESEARCH PROJECTS

Job & Internship:

- Post-doc Researcher in State University of New York at Buffalo 09/2012 – current
- Teaching assistant in University of Tartu, Estonia 07/2011 – 08/2012
- Researcher in Cybernetica AS, Estonia 09/2009 - 06/2011
- Internship in Centre for Information & Security Systems Research of British Telecommunications plc, UK 11/2008 - 03/2009
- Part-time Research Associate in Information Retrieval in UCL 04/2008 - 11/2008
- Internship in The Zhejiang Province Advanced People's Court. 3 months in 2007

Some Projects:

- Member of SHAREMIND project, which is part of Defense Advanced Research Projects Agency (DARPA) project. (Website: http://sharemind.cyber.ee/)
- Member of EU project MASTER-FP7 (Managing Assurance, Security and Trust for Services), and my work mainly focus on "Protection and Assessment workbench", doing risk modeling with GMF, OCL, etc.
- Member of 'The Platform Research Based on WEB for Product Innovation and Exploitation, and Its Application in Protocol Industry' (No.2003C11042), a key project in the Science and Technology Department of Zhejiang Province
- Principal of the project 'Early Alzheimer Intelligent Diagnosis System Based on WEB', the 3rd Prize in the 'Canal Cup' Collegiate Scientific Works Contest in our university

PERSONAL DETAILS

Date of Birth:	14 December 1984
Nationality:	Chinese
Marital Status:	Single
Language:	English (Professional), Chinese (Native)

PUBLICATIONS

1. Lipmaa, H., Zhang, B.: Efficient Generalized Selective Private Function Evaluation with Applications in Biometric Authentication. Inscrypt '09. LNCS, vol. 6151, pp. 154–163.
2. Lipmaa, H., Zhang, B.: Two New Efficient PIR-Writing Protocols. ACNS '10. LNCS, vol. 6123, pp. 438–455.
3. Zhang, B.: Generic Constant-Round Oblivious Sorting Algorithm for MPC. ProvSec '11. LNCS, vol. 6980, pp. 240–256.
4. Zhang, B.: Simulatable Adaptive Oblivious Transfer With Statistical Receiver's Privacy. ProvSec '11. LNCS, vol. 6980, pp. 52–67.
5. Laur, S., Willemson, J., Zhang, B.: Round-efficient Oblivious Database Manipulation. ISC '11. LNCS, vol. 7001, pp. 262–277.
6. Nakahara, J., Sepehrdad, P., Zhang, B., Wang, M.: Linear (Hull) and Algebraic Cryptanalysis of the Block Cipher PRESENT. CANS '09. LNCS, vol. 5888, pp. 58–75.
7. Bard, G. V., Courtois, N., Nakahara, J., Sepehrdad, P., Zhang, B.: Algebraic, AIDA/Cube and Side Channel Analysis of KATAN Family of Block Ciphers. INDOCRYPT '10. LNCS, vol. 6498, pp. 176–196.
8. Chaabouni, R., Lipmaa, H., Zhang, B.: A Non-Interactive Range Proof with Constant Communication. Financial Cryptography and Data Security 2012. LNCS.

Additional Information

About Master at UCL: avg. grade "A" (70%+); thesis title is "Fuzzy Private Matching and Privacy Preserving Information Retrieval"; supervisor is Jens Groth.

About PhD at UT: avg. grade "A" (91%+); thesis title is "Efficient Cryptographic Protocols for Secure and Private Remote Databases"; supervisors are Helger Lipmaa and Peeter Laud; opponents are Jens Groth and Jesper Buus Nielsen.