Bingsheng Zhang

State University of New York at Buffalo, 301 Davis Hall
Buffalo, New York 14260-2000, USA
Mobile: +1 (716) 263-8677
Email: b.zhang2009@gmail.com

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, Dr. 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. Dr. Zhang has strong independent R&D capability and feels confidence in both academic research and practical implementation.

EDUCATION

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

QUALIFICATIONS AND CERTIFICATIONS

- Ph.D. in Computer Science 2011
- M.sc. 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:

- Postdoctoral research associate at State University of New York, Buffalo, USA 09/2012- current
- Teacher at University of Tartu, Estonia 07/2011 - 08/2012
- Researcher at Cybernetica AS, Estonia 09/2009 - 06/2011
- Paid Internship at Centre for Information & Security Systems Research of British Telecommunications plc, UK 11/2008 - 03/2009
- Part-time Research Associate in Information Retrieval in UCL, UK 04/2008 - 11/2008
- Internship in The Zhejiang Province Advanced People's Court, China 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: Married
Language: English (Professional), Chinese (Native)

PUBLICATIONS

1. **[NDSS'13 ShortTalk]** OIRS: Outsourced Image Recovery Service from Compressive Sensing with Privacy Assurance, NDSS'13, Short Talks, with C. Wang, X. Zhen, K. Ren, and J. Wang.
2. **[FC'13]** Practical Fully Simulatable Oblivious Transfer with Sublinear Communication, FC'13, with H. Lipmaa, C. Wang, and K. Ren.
3. **[SCN'12]** A More Efficient Computationally Sound Non-Interactive Zero-Knowledge Shuffle Argument, SCN'12, with H. Lipmaa.
4. **[FC'12]** A Non-interactive Range Proof with Constant Communication, FC'12, with R. Chaabouni, and H. Lipmaa.
5. **[ISC'11]** Round-Efficient Oblivious Database Manipulation, ISC'11, with S. Laur, and J. Willemson.
6. **[ProvSec'11]** Generic Constant-Round Oblivious Sorting Algorithm for MPC, ProvSec'11.
7. **[ProvSec'11]** Simulatable Adaptive Oblivious Transfer With Statistical Receiver's Privacy, ProvSec'11.
8. **[INDOCRYPT'10]** Algebraic, AIDA/Cube and Side Channel Analysis of KATAN Family of Block Ciphers, INDOCRYPT`10 with G. Bard, N. Courtois, J. Nakahara, and P. Sepehrdad.
9. **[ACNS'10]** Two New Efficient PIR-Writing Protocols, ACNS`10, with H. Lipmaa.
10. **[CANS'09]** Linear (Hull) and Algebraic Cryptanalysis of the Block Cipher PRESENT, CANS'09, with J. Nakahara, P. Sepehrdad, and M. Wang.
11. **[Inscrypt'09]** Efficient Generalized Selective Private Function Evaluation with Applications in Biometric Authentication, Inscrypt'09, with H. Lipmaa.