Kaitai Liang
Curriculum Vitae

Post-doctoral Researcher (Ph.D.)
Department of Computer Science
School of Science
Aalto University, Finland
Email : kaitai.liang@aalto.fi
Phone: +358 50 4301157

Objective and Research Interests

My primary research interests are cybersecurity, privacy and security in information technology; in particular, security in big data analysis, privacy in Internet of things, cloud security, privacy enhancing technology and lightweight secure systems. With additional experience and background on software engineering and knowledge of security, my objective is to conduct innovative researches, developing practical secure systems, exploring applications of information security for university and governmental institution.

Education

- From **Sep. 2014 to Present**, Post-doc,
Dept. of Computer Science, Aalto University (under Prof. Kaisa Nyberg), Espoo, Finland
- From **Sep. 2011 to Aug. 2014**, PhD, Computer Science (Cryptography direction),
City University of Hong Kong (CityU) (under Dr. Duncan S. Wong), Hong Kong
- From **Sep. 2008 to June 2011**, M.Sc., Computer Applied Technology,
South China Agricultural University (SCAU) (under Prof. Bo Yang), China
- From **Sep. 2004 to July 2008**, B.Eng., Software Engineering,
South China Agricultural University, China

Working/Visiting Experiences

- From **Sep. 2014 to Present**: Post-Doc, Dept. of Computer Science, Aalto University, Finland.
- **Jan. 2016**: Academic Visit, Prof. Mauro Conti, SPRITZ**,** University of Padua, Italy**.**
- **Dec. 2015**: Academic Visit, Dr. Claudia Diaz, COSIC, KU LEUVEN, Belgium.
- From **Sep. 2015 to Nov. 2015**: Academic Visit, Prof. Giuseppe Ateniese, security group, Dept. of Computer Science, Sapienza University of Rome, Italy.
- From **Mar. 2015 to June 2015**: Academic Visit, Prof. Chris Mitchell, Information security group, Royal Holloway, University of London; Dr. Liqun Chen, HP Lab Bristol; Prof. Mark Ryan, security group, University of Birmingham; Dr. Feng Hao, Dept. of Computer Science, Newcastle University; Dr. Emiliano D.C., Dept. of Computer Science, University College London, UK.
- From **Dec. 2013 to June 2014**: Research Intern, Institute for Infocomm Research (I2R), A*STAR, Singapore.
- From **June 2013 to Nov. 2013**: Academic Visit, University of Wollongong, Australia.
- From **Sep. 2011 to Sep. 2013**: Teaching Assistant, Dept. of Computer Science, CityU, Hong Kong.
- From **Sep. 2008 to Aug. 2009**: Teaching Assistant, SCAU, China.
- From **Sep. 2007 to Dec. 2007**: Software Develop Intern, ChinaSoft International Limited, China.

Professional Activities

International/National/Industrial Projects Involved as Key Member

1. Privacy-aware retrieval and modelling of genomic data (PRIGENDA), Academy of Finland (No. 13283250).
2. Secure Data Sharing in Cloud Computing Environment (No. SecDC-112172014), Institute for Infocomm Research, A*STAR, Singapore.
3. Practical Unified Framework for Secure E-Consent Mechanism for Health Records (No. LP120200052), Australian Research Council Linkage Project, Australia.
4. On the Theory and Application of Attribute-Based Cryptography (No. 123511), Research Grants Council of Hong Kong.
5. Secure and Efficient Optimistic Fair Exchange Protocols (No. 61103232), National Natural Science Foundation of China.
6. Secure Multiparty Computational Geometry (No. 60973134), National Natural Science Foundation of China.
7. Biometric Data based Key Management (No. 60773175), National Natural Science Foundation of China.
8. Sensitive Information Protection in Trusted Network (No. 9140C1108020906), Foundation of National Laboratory for Modern Communications.
9. Industrial Email System Development (Java), Information Management System (Java), ChinaSoft International Limited, China.

Program Committee

1. The 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom 2015), Program Committee.
2. The 1st International Workshop on Cyber Security (CS 2015), Program Committee.
3. The 11th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2016), Publication Chair.
4. The 21st Australasian Conference on Information Security and Privacy (ACISP 2016), Program Committee and publication chair.
5. The 10th International Conference on Provable Security (ProvSec 2016), Program Committee.
6. The 10th International Conference on Network and System Security (NSS 2016), Program Committee.
7. The 15th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom 2016), Program Committee.
8. The 23rd Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2017), Organization Committee.

Invited Talks/Seminars

1. (Talk) Privacy-preserving and expressive encrypted data share/search, Colloquia and Seminars, Dept. of Computer Science, Newcastle University, UK, 28th May, 2015;
2. (Talk) Encrypted cloud-based data sharing, Computer Security seminar, School of Computer Science - Security and Privacy Group, University of Birmingham, UK, 4th June, 2015;
3. (Talk) Could we share and search our cloud data in an efficient and privacy-preserving way? Dept. of Computer Science, City University of Hong Kong, Hong Kong, 7th July, 2015;
4. (Talk) How to share and search our encrypted cloud-based data without loss of privacy, Division of Communication Engineering, Nanyang Technological University, Singapore, 10th July, 2015; Secure Mobile Centre, Singapore Management University, Singapore, 9th July, 2015;

5. (Talk) Privacy-preserving relatedness test, Miyaji Lab, Japan Advanced Institute of Science and Technology, Japan, 9th Sep., 2015;
6. (Talk) Secure data search, share & Genomic Privacy, Security Group, Dept. of Computer Science, Sapienza University of Rome, Italy, 2nd Nov., 2015;
7. (Talk) Outsourced Personal Data – Secure Share, Search and More, COSIC seminar, KU LEUVEN, 16th Dec., 2015; Safety and Security Department, Austrian Institute of Technology, 26th April, 2016;
8. (Talk) Some Privacy and Security Issues in Online Social Networks, SPRITZ research group, Dept. of Mathematics**,** University of Padua, Italy, 28th Jan., 2016.
9. (Seminar) Genomic privacy, Dagstuhl Seminar, Schloss Dagstuhl, Germany, 18th - 23rd Oct., 2015.

Teaching Experiences

1. 2015, T-79.4502 - Cryptography and Data Security, master course, Aalto University, Finland
2. 2012/13, CS1302 Introduction to Computer Programming, CityU
3. 2011/12, CS3391 Advanced Programming, CityU
4. 2011/12, CS3342 Software Design, CityU

Awards

1.	Post-doc researcher funding, Academic of Finland, € 227,481	2016
2.	Austrian researchers Career Grants (interview grant), Austria	2016
3.	COST Crypto Action IC1306 academic visiting fund, € 2,500, Europe	Sep. to Nov. 2015
4.	Best research paper award, European Symposium on Research in Computer Security,	Sep. 2015
5.	Ph.D. Scholarship, HKD$14,400/month, CityU, Hong Kong	2011 to 2014
6.	Research Activities Fund, HKD$25,000, CityU, Hong Kong	June to Dec. 2013
7.	Certificate of Merit in the Teaching Students: Fist Steps Course, CityU, Hong Kong	Mar. 2013
8.	Conference Grant (ICISC 2012), HKD$6,485, CityU, Hong Kong	Dec. 2012
9.	Scientific and Technological Innovation Honor, SCAU, China	Dec. 2010
10.	Outstanding Postgraduate Student, Minor Award, SCAU, China	June 2010
11.	Outstanding Postgraduate Student, Major Award, SCAU, China	May 2009
12.	Outstanding Graduate, SCAU, China	June 2008
13.	Outstanding Undergraduate, Major Award, SCAU, China	May 2008
14.	Excellent Individual on Software Development, ChinaSoft International Limited,	Dec. 2007
15.	Outstanding Undergraduate, Minor Award, SCAU, China	Dec. 2007
16.	Outstanding Undergraduate, Minor Award, SCAU, China	Dec. 2006
17.	Outstanding Undergraduate, Minor Award, SCAU, China	Nov. 2005

Publications

Journal Papers

1. Joseph K. Liu, Man Ho Au, Willy Susilo, **Kaitai Liang**, and Rongxing Lu, "Secure Sharing and Searching for Real-Time Video Data in Mobile Cloud," ***IEEE Network Magazine*** 29(2): 46-50 (2015), impact factor: 2.54.
2. **Kaitai Liang**, Willy Susilo, "Searchable Attribute-Based Mechanism with Efficient Data Sharing for Secure Cloud Storage," ***IEEE Transactions on Information Forensics and Security*** 10(9): 1981-1992 (2015), impact factor: 2.408.
3. **Kaitai Liang**, Willy Susilo, Joseph K. Liu, "Privacy-Preserving Ciphertext Sharing Mechanism for Big Data Storage," ***IEEE Transactions on Information Forensics and Security*** 10(8): 1578-1589 (2015), impact factor: 2.408.
4. Rongxing Lu, Xiaodong Lin, Jun Shao, **Kaitai Liang** "Secure Bidirectional Proxy Re-Encryption for Cryptographic Cloud Storage," (accepted, June 2015, ***Pervasive and Mobile Computing***, impact factor: 2.079)
5. **Kaitai Liang**, Joseph K. Liu, Rongxing Lu, Duncan S. Wong, "Privacy Concerns for Photo-Sharing in Online Social Networks," ***IEEE Internet Computing*** 19(2): 58-63 (2015), impact factor: 1.713.
6. Joseph K. Liu, **Kaitai Liang**, Willy Susilo, Jianghua Liu, Yang Xiang, "Two-Factor Data Security Protection Mechanism for Cloud Storage System," (accepted, June 2015, ***IEEE Transactions on Computers***, impact factor: 1.659)
7. Xinyi Huang, Joseph K. Liu, Shaohua Tang, Yang Xiang, **Kaitai Liang**, Li Xu, Jianying Zhou, "Cost-Effective Authentic and Anonymous Data Sharing with Forward Security," ***IEEE Transactions on Computers*** 64(4): 971-983 (2015), impact factor: 1.659.
8. **Kaitai Liang**, Liming Fang, Duncan S. Wong, and Willy Susilo, "A Ciphertext-Policy Attribute-Based Proxy Re-Encryption with Chosen-Ciphertext Security," ***Concurrency and Computation Practice and Experience*** 27(8): 2004-2027 (2015), impact factor: 0.997.
9. **Kaitai Liang**, Willy Susilo, Joseph K. Liu, Duncan S. Wong, "Efficient and Fully CCA Secure Conditional Proxy Re-Encryption from Hierarchical Identity-Based Encryption," ***Computer Journal*** 58(10): 2778-2792 (2015), impact factor: 0.787.
10. Jiannan Wei, Guomin Yang, Yi Mu, **Kaitai Liang**, "Anonymous Proxy Signature with Hierarchical Traceability," (accepted, April 2015, ***Computer Journal***, impact factor: 0.787)
11. Anjia Yang, **Kaitai Liang**, Yunhui Zhuang, Duncan S. Wong, and Xiaohua Jia, "A new unpredictability-based radio frequency identification forward privacy model and a provably secure construction," ***Security and Communication Networks*** 8(16): 2836-2849 (2015), impact factor: 0.720
12. **Kaitai Liang**, Man Ho Au, Joseph K. Liu, Willy Susilo, Duncan S. Wong, Guomin Yang, Yong Yu, Anjia Yang, "A Secure and Efficient Ciphertext-Policy Attribute-Based Proxy Re-Encryption for Cloud Data Sharing," (In Press, Available online 03/12/2014, ***Future Generation Computer Systems***, impact factor: 2.786)
13. **Kaitai Liang,** Man Ho Au, Joseph K. Liu, Willy Susilo, Duncan S. Wong, Guomin Yang, Tran Viet Xuan Phuong, Qi Xie, "A DFA-Based Functional Proxy Re-Encryption Scheme for Secure Public Cloud Data Sharing," ***IEEE Transactions on Information Forensics and Security*** 9(10): 1667-1680 (2014), impact factor: 2.408.
14. **Kaitai Liang**, Cheng-Kang Chu, Xiao Tan, Duncan S. Wong, Chunming Tang, and Jianying Zhou, "Chosen-Ciphertext Secure Multi-Hop Identity-Based Conditional Proxy Re-Encryption with Constant-Size Ciphertexts," ***Theoretical Computer Science***, Volume 539, 19 June 2014, Pages 87-105, impact factor: 0.657.
15. Clementine Gritti, Willy Susilo, Thomas Plantard, **Kaitai Lang** and Duncan S. Wong, "Broadcast Encryption with Dealership," (in press, ***International Journal of Information Security***, impact factor: 0.963)

16. Clementine Gritti, Willy Susilo, Thomas Plantard, **Kaitai Liang**, "Empowering Personal Health Records with Cloud Computing – How to Encrypt with Forthcoming Fine Grain Policies Efficiently," (to appear, ***Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications***)
17. Shulan Wang, **Kaitai Liang**, Joseph K. Liu, Jianping Yu, Jianyong Chen, "Improving Security and Attribute Expression of Data Sharing Scheme in Cloud Computing," (accepted, ***IEEE Transactions on Information Forensics and Security***, impact factor: 2.408)
18. **KaitaiLiang**, XinyiHuang, FuchunGuo, Joseph K. Liu, "Privacy-Preserving and Regular Language Search over Encrypted Cloud Data," (accepted, ***IEEE Transactions on Information Forensics and Security***, impact factor: 2.408)
19. **Kaitai Liang**, Duncan S. Wong, Willy Susilo, "Amelioration on a Functional Proxy Re-Encryption System for Public Cloud Data Sharing," (Major Revision, ***IET Information Security***, impact factor: 0.753)

Conference Papers

20. **Kaitai Liang**, Atsuko Miyaji and Chunhua Su, "Secure and Traceable Framework for Data Circulation", 21st Australasian Conference on Information Security and Privacy (ACISP 2016), accepted.
21. Peng Zhang, Zehong Chen, **Kaitai Liang**, Shulan Wang, Ting Wang, "A Cloud-Based Access Control Scheme with User Revocation and Attribute Update", 21st Australasian Conference on Information Security and Privacy (ACISP 2016), accepted.
22. Tran Viet Xuan Phuong, Guomin Yang, Willy Susilo, **Kaitai Liang**, "Edit Distance Based Encryption and Its Application", 21st Australasian Conference on Information Security and Privacy (ACISP) 2016, accepted.
23. **Kaitai Liang**, Chunhua Su, Jiageng Chen, Joseph K. Liu, "Efficient Multi-Function Data Sharing and Searching Mechanism for Cloud-Based Encrypted Data", 11th ACM Asia Conference on Computer and Communications Security (AsiaCCS 2016), accepted.
24. Shangqi Lai, Joseph K. Liu, Kim-Kwang Raymond Choo and **Kaitai Liang**, "Secret Picture: An Efficient Tool for Mitigating Deletion Delay on OSN," 17th International Conference on Information and Communications Security (ICICS 2015), Lecture Notes in Computer Science 9543, pp. 467-477, Springer, December 2015.
25. Yanjiang Yang, Joseph K. Liu, **Kaitai Liang**, Raymond Choo, Jianying Zhou, "Extended Proxy-Assisted Approach: Achieving Revocable Fine-Grained Cloud Data Encryption," in Proc. of the 20th European Symposium on Research in Computer Security (ESORICS 2015), Lecture Notes in Computer Science 9327, pp. 146-166, Springer, November 2015, **best research paper award**.
26. **Kaitai Liang**, Joseph K. Liu, Duncan S. Wong and Willy Susilo, "An Efficient Cloud-based Revocable Identity-based Proxy Re-encryption Scheme for Public Clouds Data Sharing," in Proc. of the 19th European Symposium on Research in Computer Security (ESORICS 2014), Lecture Notes in Computer Science 8712, pp. 257-272, Springer, September 2014.
27. Rongxing Lu, Xiaodong Lin, Jun Shao, and **Kaitai Liang**, "RCCA-Secure Multi-use Bidirectional Proxy Re-Encryption with Master Secret Security," in Proc. of the 8th International Conference on Provable Security (ProvSec 2014), Lecture Notes in Computer Science 8782, pp. 194-205, Springer, October 2014.
28. **Kaitai Liang**, Man Ho Au, Willy Susilo, Duncan S. Wong, Guomin Yang, and Yong Yu, "An Adaptive CCA-Secure Ciphertext-Policy Attribute-Based Proxy Re-Encryption for Cloud Data Sharing", in Proc. of the 10th Information Security Practice and Experience Conference (ISPEC 2014), Lecture Notes in Computer Science 8434, pp. 448-461, Springer, May 2014.
29. **Kaitai Liang**, Qiong Huang, Roman Schlegel, Duncan S. Wong, and Chunming Tang, "A Conditional Proxy Broadcast Re-Encryption Scheme Supporting Timed-Release," in Proc. of the 9th Information Security Practice and Experience Conference (ISPEC 2013), Lecture Notes in Computer Science 7863, pp. 132-146, Springer, May 2013.

30. **Kaitai Liang**, Liming Fang, Duncan S. Wong, and Willy Susilo, "A Ciphertext-Policy Attribute-Based Proxy Re-Encryption with Chosen-Ciphertext Security," in Proc. of the 5th International Conference on Intelligent Networking and Collaborative Systems (INCoS 2013).
31. **Kaitai Liang**, Zhen Liu, Xiao Tan, Duncan S. Wong, and Chunming Tang, "A CCA-Secure Identity-Based Conditional Proxy Re-Encryption without Random Oracles," In Proc. of the 15th International Conference on Information Security and Cryptology (ICISC 2012), Lecture Notes in Computer Science 7839, pp. 231-246, Springer, 2012.

References

Prof. Kaisa Nyberg (Post-doc supervisor)
Leader, Cryptography Group, Department of Computer Science,
Aalto University, Finland
kaisa.nyberg@aalto.fi

Dr. Duncan S. Wong (Ph.D. supervisor)
Director, Exploratory Research Laboratory,
Hong Kong Applied Science and Technology Research Institute, Hong Kong
duncanwong@astri.org

Prof. Willy Susilo (Academic Collaborator)
ARC Future Fellow, Head of School of Computing and Information Technology,
Co-Director, Centre for Computer and Information Security Research,
University of Wollongong, Australia
wsusilo@uow.edu.au