# Curriculum Vitae

## Personal Information


Name: Lei Zhang  Gender: Male

Nationality: China  Email: leizhang@sei.ecnu.edu.cn

Current Address: Science Building, No. 3663 Zhongshan Road (North), Shanghai 200062, P. R. China


**Lei Zhang** received his Ph.D. degree in computer engineering from Universitat Rovira i Virgili, Tarragona, Spain. Since then, he has been with Universitat Rovira i Virgili, Tarragona, Spain, as a Postdoctoral Researcher. He was a visiting student in Cryptology Research Group, Centrum Wiskunde & Informatica (CWI). He is currently a full Professor with the School of Computer Science and Software Engineering, East China Normal University, Shanghai, China. He has been a holder/co-holder of more than 10 China/Spain-funded (key) projects. His fields of activity are information security, cryptography, VANET security, cloud security and data privacy. He has authored over 60 publications, including: IEEE Transactions on Computers, IEEE Transactions on Information Forensics and Security, IEEE Transactions on Intelligent Transportation Systems, IEEE Transactions on Vehicular Technology, IEEE-ACM Transactions on Networking, ESORICS 2014, ASIACRYPT 2011. He is the editors of several international journals. He has served in the program committee of more than 20 international conferences, in the steering committee of 2 international conferences, and as a technical reviewer for over 30 major scientific journals in information security and privacy. He is a member of IEEE.

## 3. Publications

### 3.1 Journal Papers (Selected)

1. Jiangtao Li, Lei Zhang, Sender Dynamic, Non-Repudiable, Privacy-Preserving and Strong Secure Group Communication Protocol, Information Sciences, DOI: 10.1016/j.ins.2017.06.003.

2. Jian Liu, Jiangtao Li, Lei Zhang, Feifei Dai, Yuanfei Zhang, Xinyu Meng, Jian Shen, Secure Intelligent Traffic Light Control Using Fog Computing, Future Generation Computer Systems, DOI: 10.1016/j.future.2017.02.017.

3. Jiangtao Li, Lei Zhang, Joseph K. Liu, Haifeng Qian, Zheming Dong, Privacy-Preserving Public Auditing Protocol for Low Performance End Devices in Cloud, IEEE Transactions on Information Forensics and Security, DOI: 10.1109/TIFS.2016.2587242

4. Lei Zhang, Qianhong Wu, Bo Qin, Hua Deng, Jiangtao Li, Jianwei Liu, Wenchang Shi,

Certificateless and Identity-based Authenticated Asymmetric Group Key Agreement, International Journal of Information Security, DOI: 10.1007/s10207-016-0339-8

5. Lei Zhang, Qianhong Wu, Josep Domingo-Ferrer, Bo Qin, Chuanyan Hu, Distributed Aggregate Privacy-Preserving Authentication in VANETs, IEEE Transactions on Intelligent Transportation Systems, DOI: 10.1109/TITS.2016.2579162.

6. Lei Zhang, Chuanyan Hu, Qianhong Wu, Josep Domingo-Ferrer, Bo Qin, Privacy-Preserving Vehicular Communication Authentication with Hierarchical Aggregation and Fast Response, IEEE Transactions on Computers, 65(8), 2562–2574, 2016

7. Qianhong Wu, Bo Qin, Lei Zhang, Josep Domingo-Ferrer, Oriol Farràs, Jesús A. Manjón, Contributory Broadcast Encryption with Efficient Encryption and Short Ciphertexts, IEEE Transactions on Computers, 65(2), 466 - 479, 2016.

8. Lei Zhang, Qianhong Wu, Bo Qin, Josep Domingo-Ferrer, Bao Liu, Practical Secure and Privacy-Preserving Scheme for Value-Added Applications in VANETs, Computer Communications, 71(2015), 50 - 60, 2015.

9. Lei Zhang, Qianhong Wu, Josep Domingo-Ferrer, Bo Qin, Zheming Dong, Round-Efficient and Sender-Unrestricted Dynamic Group Key Agreement Protocol for Secure Group Communications, IEEE Transactions on Information Forensics and Security, 10(11), 2352-2364, 2015.

10. Lei Zhang, Certificateless One-Pass and Two-Party Authenticated Key Agreement Protocol and Its Extensions, Information Sciences, 293(2015), 182-195, 2015.

11. Lei Zhang, Qianhong Wu, Josep Domingo-Ferrer, Bo Qin, Peng Zeng, Signatures in Hierarchical Certificateless Cryptography: Efficient Constructions and Provable Security, Information Sciences, 272 (2014), 223–237, 2014.

12. Hua Deng, Qianhong Wu, Bo Qin, Josep Domingo-Ferrer, Lei Zhang, Jianwei Liu, Wenchang Shi, Ciphertext-Policy Hierarchical Attribute-Based Encryption with Short Ciphertexts, Information Sciences, 275(2014), 370–384, 2014.

13. Lei Zhang, Qianhong Wu, Bo Qin, Identity-Based Optimistic Fair Exchange in the Standard Model, Security and Communication Networks, 6(8), 1010–1020, 2013.

14. Qianhong Wu, Bo Qin, Lei Zhang, Josep Domingo-Ferrer, Fast Transmission to Remote Cooperative Groups: A New Key Management Paradigm, IEEE-ACM Transactions on Networking, 21(2), 621-633, 2013.

15. Bo Qin, Qianhong Wu, Lei Zhang, Oriol Farras, Josep Domingo-Ferrer, Provably Secure Threshold Public-Key Encryption with Adaptive Security and Short Ciphertexts, Information Sciences, 210(2012), 67–80, 2012.

16. Lei Zhang, Futai Zhang, Qianhong Wu, Delegation of Signing Rights using Certificateless Proxy Signatures, Information Sciences, 184(1), 298-309, 2012.

17. Lei Zhang, Qianhong Wu, Bo Qin, Josep Domingo-Ferrer, Úrsula González-Nicolás,

Asymmetric Group Key Agreement Protocol for Open Networks and Its Application to Broadcast Encryption, Computer Networks, 55(15), 3246–3255, 2011.

18. Lei Zhang, Qianhong Wu, Bo Qin, Josep Domingo-Ferrer. Provably Secure One-Round Identity-Based Authenticated Asymmetric Group Key Agreement Protocol, Information Sciences, 181(19), 4318-4329, 2011.

19. Lei Zhang, Bo Qin, Qianhong Wu, Futai Zhang. Efficient Many-to-One Authentication with Certificateless Aggregate Signatures, Computer Networks, 54(14), 2482–2491, 2010.

20. Lei Zhang, Qianhong Wu, Agusti Solanas, Josep Domingo-Ferrer. A Scalable Robust Authentication Protocol for Secure Vehicular Communications, IEEE Transactions on Vehicular Technology, 59(4), 1606–1617, 2010.

21. Lei Zhang, Futai Zhang, Qianhong Wu, Josep Domingo-Ferrer. Simulatable Certificateless Two-Party Authenticated Key Agreement Protocol, Information Sciences, 180(6), 1020–1030, 2010.

22. Lei Zhang, Futai Zhang. A New Certificateless Aggregate Signature Scheme, Computer Communications, 32(6), 1079-1085, 2009.

## Conference Papers (selected)

1. Hua Deng, Qianhong Wu, Bo Qin, Jian Mao, Xiao Liu, Lei Zhang and Wenchang Shi, Who Is Touching My Cloud, the 19th European Symposium on Research in Computer Security (ESORICS 2014), vol. 8712, pp. 362–379, 2014.

2. Zheming Dong, Lei Zhang, Jiangtao Li, Security Enhanced Anonymous Remote User Authentication and Key Agreement for Cloud Computing, 17th International Conference on Computational Science and Engineering (CSE 2014), IEEE, pp. 1746-1751, 2014.

3. Lei Zhang, Qianhong Wu, Bo Qin, Hua Deng, Jianwei Liu, Wenchang Shi, Provably Secure Certificateless Authenticated Asymmetric Group Key Agreement, The 10th International Conference on Information Security Practice and Experience (ISPEC 2014), vol. 8434, pp. 496–510, 2014.

4. Lei Zhang, Qianhong Wu, Josep Domingo-Ferrer, Bo Qin, Sherman S. M. Chow, Wenchang Shi, Secure One-to-Group Communications: Escrow-Free ID-Based Asymmetric Group Key Agreement, 9th China International Conference on Information Security and Cryptology (INSCRYPT 2013), vol. 8567, pp. 239-254, 2014.

5. Lei Zhang, Qianhong Wu, Bo Qin, Josep Domingo-Ferrer, Peng Zeng, Jianwei Liu, Ruiying Du, A Generic Construction of Proxy Signatures from Certificateless Signatures, The 27th IEEE International Conference on Advanced Information Networking and Applications (AINA 2013), IEEE, pp. 259 – 266, 2013.

6. Lei Zhang, Provably Secure Certificateless One-Way and Two-Party Authenticated Key Agreement Protocol, The 15th Annual International Conference on Information Security and Cryptology (ICISC 2012), vol. 7839, pp 217-230, Springer-Verlag, 2013.

7. Qianhong Wu, Bo Qin, Lei Zhang, Josep Domingo-Ferrer, Oriol Farras, Bridging Broadcast Encryption and Group Key Agreement, The 17th Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2011), vol. 7073, pp. 143-160, Springer-Verlag, 2011.

8. Lei Zhang, Qianhong Wu, Bo Qin, Josep Domingo-Ferrer, APPA: Aggregate Privacy-Preserving Authentication in Vehicular Ad Hoc Networks, The 14th Information Security Conference (ISC 2011), vol. 7001, pp. 293-308, Springer-Verlag, 2011.

9. Lei Zhang, Qianhong Wu, Josep Domingo-Ferrer, Bo Qin, Hierarchical Certificateless Signatures, Sixth IEEE/IFIP International Symposium on Trusted Computing and Communications (TrustCom-10), IEEE, pp. 572-577, 2010.

10. Qianhong Wu, Bo Qin, Lei Zhang, Josep Domingo-Ferrer. Ad Hoc Broadcast Encryption (Extended Abstract), ACM Conference on Computer and Communications Security (ACM CCS 2010), ACM, pp. 741-743, 2010.

11. Lei Zhang, Qianhong Wu, Bo Qin, Josep Domingo-Ferrer. Identity-Based Authenticated Asymmetric Group Key Agreement Protocol, The 16th Annual International Computing and Combinatorics Conference (COCOON 2010), vol. 6196, pp. 510-519, Springer-Verlag, 2010.

12. Lei Zhang, Qianhong Wu, Bo Qin. Authenticated Asymmetric Group Key Agreement Protocol and Its Application, 2010 IEEE International Conference on Communications (ICC 2010), IEEE, pp. 1-5, 2010.

13. Lei Zhang, Futai Zhang. A New Provably Secure Certificateless Signature Scheme, 2008 IEEE International Conference on Communications (ICC 2008), IEEE, pp. 1685-1689, 2008.