Yu Chen ✉: cycosmic@gmail.com ☎: (+86)-135 8163 6429

Research Interest

Cryptography in general with focus on

- Fundamental primitives and reduction techniques
- Cryptographic schemes with advanced functionality and security
- Zero-knowledge proof systems and applications

Experience

Post-Doctoral Fellow (working with Prof. Sherman S.M. Chow) 2015.08 - 2016.01
Crypto Group, Department of Information Engineering, The Chinese University of Hong Kong

Associate Professor (PhD Supervisor) 2013.10 - 2019.06
Assistant Professor 2011.07 - 2013.10
State Key Lab of Information Security, Institute of Information Engineering, Chinese Academy of Sciences
School of Cyber Security, Chinese Academy of Sciences

Senior Technical Expert 2019.06 - 2019.12
Ant Financial

Professor 2019.12 - Present
School of Cyber Science and Technology, Shandong University

Education

Ph.D. Computer Software and Theory, Peking University, Beijing, China 2006.09 - 2011.07
GPA (major) 87/100 Top 10%

Joint Ph.D. Program, School of Computing, Dublin City University, Ireland 2009.09 - 2010.10
Jointly supervised by Prof. Michael Scott and Prof. Liqun Chen.

B.E. Information Security, Hefei University of Technology, Hefei, China 2002.09 - 2006.07
GPA (major) 90/100 Rank 1st/49

Honors and Awards

Guanghua Scholarship, Peking University (Top 5%)	2010
Special Scholarship on Study, Peking University (Top 10%)	2008, 2010
Award of Outstanding Graduate of Anhui Province (Top 1%)	2006
Honorable Mention in American Undergraduate Mathematical Contest in Modeling	2005
Top Class Scholarship, Hefei University of Technology (Top 1%)	2002, 2004
First Class Scholarship, Hefei University of Technology (Top 2%)	2003

Academic Service

External Reviewer: Asiacrypt (2012, 2013, 2016, 2017), PKC 2018

Program Committee Member: Inscrypt 2014, Provsec 2016, CANS 2017

Research Funding

National Natural Science Foundation of China 2018.01-2021.12
Key-Dependent Message Security for Identity-Based Encryption, Grant No.61772522

National Natural Science Foundation of China — 2014.01-2016.12
Leakage-Resilient Functional Encryption, Grant No.61303257

Youth Innovation Promotion Association CAS — 2017.01-2020.12

Young Star Talents Planning, Institute of Information Engineering, CAS — 2014.01-2016.12

Teaching (UCAS)

Theoretical Foundations of Cryptography — 2017, 2018

Advanced Cryptographic Tools and Primitives — 2018, 2019

Awards

- 2018 China Cryptography Innovation Award (Second Prize)

CCF Rank **CACR Rank**

Refereed Journal Articles (Selected)

1. Binbin Tu, **Yu Chen***, Xueli Wang. Threshold Trapdoor Functions and Their Applications. *IET Information Security*, Vol.14(2), 2020, pp.220-231.

2. Binbin Tu, **Yu Chen***. A Survey of Threshold Cryptosystems. *Journal of Cryptologic Research*, Vol. 7(1), 2020, pp.1–14.

3. **Yu Chen**, Jiang Zhang, Yi Deng, Jinyong Chang. KDM Security for IBE: Generic Constructions and Separations. *Information Sciences*, Vol. 486, 2019, pp. 450-473. (CCF B)

4. **Yu Chen**, Baodong Qin, Haiyang Xue. Regular Lossy Functions and Their Applications in Leakage-Resilient Cryptography. *Theoretical Computer Science*, Vol.739, 2018, pp.13-38. A preliminary version of this paper appears in CT-RSA 2018. (CCF B)

5. **Yu Chen**, Zongyang Zhang. Publicly Evaluable Pseudorandom Functions and Their Applications. *Journal of Computer Security*, Vol.24(2), 2016, pp.289-320. A preliminary version of this paper appears in SCN 2014. (CCF B)

6. **Yu Chen**, Qiong Huang, Zongyang Zhang. Sakai-Ohgishi-Kasahara Identity-Based Non-Interactive Key Exchange Revisited and More. *International Journal of Information Security*, Vol.15(1), 2016, pp.15-33. A preliminary version of this paper appears in ACISP 2014. (CACR B)

7. **Yu Chen**, Jiang Zhang, Dongdai Lin, Zhenfeng Zhang. Generic Constructions of Integrated PKE and PEKS. *Designs, Codes and Cryptography*, Vol.78(2), 2016, pp.493-526. (CCF B)

8. Jiang Zhang, Zhenfeng Zhang, **Yu Chen**. PRE: Stronger Security Notions and Efficient Construction with Non-interactive Opening. *Theoretical Computer Science*, Vol.542, 2014, pp.1-16. (CCF B)

9. **Yu Chen**, Liqun Chen, Dongdai Lin. Reflections on the Security Proofs of Boneh-Franklin Identity-Based Encryption Scheme. *Science China Mathematics*, Vol.56(7), 2013, pp.1385-1401. (CCF C)

10. **Yu Chen**, Zongyang Zhang, Dongdai Lin, Zhenfu Cao. Generalized (Identity-Based) Hash Proof System and Its Applications. *Security and Communication Networks*, Vol.9(12), 2016, pp.1698-1716. A preliminary version of this paper appears in Provsec 2012. (CCF C)

11. **Yu Chen**, Zongyang Zhang, Dongdai Lin, Zhenfu Cao. CCA-Secure IB-KEM from Identity-Based Extractable Hash Proof System. *The Computer Journal*, Vol.57(10), 2014, pp.1537-1556. A preliminary version of this paper appears in ACNS 2012. (CCF B)

12. Liqun Chen, **Yu Chen**. The n-Diffie-Hellman Problem and Multiple-Key Encryption. *International Journal of Information Security*, Vol.11, No.5, 2012, pp.305-320. A preliminary version of this paper appears in ISC 2011. (CACR B)

Refereed Conference Papers (Selected)

1. Xueli Wang, **Yu Chen***, Xuecheng Ma. Adding Linkability to Ring Signatures with One-Time Signatures. *ISC 2019.*

2. **Yu Chen**, Yuyu Wang, Hong-Sheng Zhou. Leakage-Resilient Cryptography from Puncturable Primitives and Obfuscation. *ASIACRYPT 2018.* (CCF B, CACR A)

3. **Yu Chen**, Baodong Qin, Haiyang Xue. Regular Lossy Functions and Their Applications. *CT-RSA 2018.* (CCF C, CACR B)

4. Zheng Yang, **Yu Chen***, Song Luo. Two-message Key Exchange with Strong Security from Ideal Lattices. *CT-RSA 2018.* (CCF C, CACR B)

5. Yi Deng, Xuyang Song, Jingyue Yu, **Yu Chen***. On the Security of Classic Protocols for Unique Witness Relations. *PKC 2018.* (CCF B)

6. Jingyue Yu, Yi Deng, **Yu Chen**. From Attack on Feige-Shamir to Construction of Oblivious Transfer. *INSCRYPT 2017.* (CACR C)

7. Baodong Qin, Shuai Han, **Yu Chen**, Shengli Liu, Zhuo Wei. How to Make the Cramer-Shoup Cryptosystem Secure Against Linear Related-Key Attacks. *INSCRYPT 2016*, pp.1-16. (CACR C)

8. Jiang Zhang, **Yu Chen***, Zhenfeng Zhang. Programmable Hash Functions from Lattices: Short Signatures and IBEs with Small Key Sizes. *CRYPTO 2016*, pp.303-332. (CCF A)

9. **Yu Chen**, Baodong Qin, Jiang Zhang, Yi Deng, Sherman S. M. Chow. Non-Malleable Functions and Their Applications. *PKC 2016*, pp.386-416. (CCF B)

10. Zongyang Zhang, **Yu Chen***, Sherman S. M. Chow, Goichiro Hanaoka, Zhenfu Cao and Yunlei Zhao. Black-Box Separations of Hash-and-Sign Signatures in the Non-Programmable Random Oracle Model. *Provsec 2015*, pp.435-454. (CACR C)

11. Jiang Zhang, Zhenfeng Zhang, **Yu Chen**, Yanfei Guo, Zongyang Zhang. Black-Box Separations for One-More (Static) CDH and Its Generalization. *ASIACRYPT 2014*, pp.366-385. (CCF B, CACR A)

12. **Yu Chen**, Zongyang Zhang. Publicly Evaluable Pseudorandom Functions and Their Applications. *The 9th Conference on Security and Cryptography for Networks, SCN 2014*, pp.115-134. (CACR C)

13. **Yu Chen**, Qiong Huang, Zongyang Zhang. Sakai-Ohgishi-Kasahara Non-Interactive Identity-Based Key Exchange Scheme, Revisited. *The 19th Australasian Conference on Information Security and Privacy, ACISP 2014*, pp.274-289. (CACR C)

14. Zongyang Zhang, **Yu Chen***, Sherman S.M. Chow, Goichiro Hanaoka, Zhenfu Cao, Yunlei Zhao. All-but-One Dual Projective Hashing and Its Applications. *The 12th International Conference on Applied Cryptography and Network Security, ACNS 2014*, pp.181-198. (CCF C)

15. **Yu Chen**, Zongyang Zhang, Dongdai Lin, Zhenfu Cao. Anonymous Identity-Based Hash Proof Systems and Their Applications. *The 6th International Conference on Provable Security, ProvSec 2012*, pp.143-160. (CACR C)

16. **Yu Chen**, Zongyang Zhang, Dongdai Lin, Zhenfu Cao. Identity-Based Extractable Hash Proofs and Their Applications. *The 10th International Conference on Applied Cryptography and Network Security, ACNS 2012*, pp.153-170. (CCF C)

17. **Yu Chen**, Liqun Chen, Zongyang Zhang. CCA-secure IB-KEM based on the Computational Bilinear Diffie-Hellman Assumption. *The 14th Annual International Conference on Information Security and Cryptology, ICISC 2011*, pp.279-301. (CACR C)

18. Liqun Chen, **Yu Chen**. The n-Diffie-Hellman Problem and Its Applications. *The 14th International Conference on Information Security, ISC 2011*, pp.119-134. (CACR C)

19. **Yu Chen**, Song Luo, Zhong Chen. A New Leakage-Resilient IBE Scheme in the Relative Leakage Model. *The 25th Annual WG 11.3 Conference on Data and Applications Security and Privacy, DBSec 2011*, pp.263-270.

20. **Yu Chen**, Song Luo, Jianbin Hu, Zhong Chen. A Novel Commutative Blinding Identity-Based Encryption Scheme. *The 4th Canada-France MITACS Workshop on Foundations & Practice of Security, FPS 2011*, pp.73-88.

21. **Yu Chen**, Liqun Chen, Zhong Chen. Generic Methods to Achieve Tighter Security Reductions for a Category of IBE Schemes. *The 7th Information Security Practice and Experience Conference, ISPEC 2011*, pp.40-54. (CACR C)

22. Song Luo, **Yu Chen**, Jianbin Hu, Zhong Chen. New Fully Secure Hierarchical Identity-Based Encryption with Constant Size Ciphertexts. *The 7th Information Security Practice and Experience Conference, ISPEC 2011*, pp.55-70. (CACR C)

23. **Yu Chen**, Liqun Chen. Twin Bilinear Diffie-Hellman Inversion Problem and Its Application. *The 13th Annual International Conference on Information Security and Cryptology, ICISC 2010*, pp.113-132. (CACR C)

24. **Yu Chen**, Hyun Sung Kim, Jianbin Hu, Zhong Chen. When ABE meets RSS. *24th Annual IFIP WG 11.3 Working Conference on Data and Applications Security, DBSec 2010*, pp.319-326.

25. **Yu Chen**, Manuel Charlemagne, Zhi Guan, Jianbin Hu, Zhong Chen. Identity-Based Encryption based on DHIES. *The 5th ACM Symposium on Information, Computer and Communications Security, ASIACCS 2010*, pp.82-88. (CACR B)