陈宇

中国科学院信息工程研究所
信息安全国家重点实验室 (第一研究室)
北京市海淀区闵庄路甲 89 号 B2 座 #3218

电话: 13581636429
邮箱: cycosmic@gmail.com
主页: https://yuchen1024.github.io

研究兴趣: 密码学

- 基本密码组件及归约技术
- 高功能高安全的密码方案设计
- 零知识证明系统、多方安全计算
- 隐私保护技术在密码货币中的应用

工作经历

- 博士后, 香港中文大学, 信息工程系 2015.08 - 2016.01
- 副研究员 (博导), 中国科学院信息工程研究所, 信息安全国家重点实验室 2013.10 - 至今
- 助理研究员, 中国科学院信息工程研究所, 信息安全国家重点实验室 2011.07 - 2013.09
- 岗位教师, 中国科学院大学, 网络空间安全学院 2017.01 - 至今

教育背景

- 理学博士 (计算机软件与理论), 北京大学, 信息科学技术学院 (导师: 陈钟) 2006.09 - 2011.07
- 博士生联合培养, 爱尔兰都柏林城市大学, 计算机系 (导师: Michael Scott) 2009.09 - 2010.08
- 工学学士 (信息安全), 合肥工业大学, 计算机与信息工程学院 2002.09 - 2006.07
  GPA: 90/100, 专业排名: 1st/49

科研项目 (主持)

- 身份加密体制的 KDM 安全研究 国家自然科学基金面上项目 (No. 61772522) 2018.01-2021.12
- 抗泄漏的函数加密体制研究 国家自然科学基金青年项目 (No. 61303257) 2014.01-2016.12
- 抗泄漏密码体制的若干关键问题研究 密码科学技术国家重点实验室面上项目 2018.07-2020.06
- 中国科学院青年创新促进会 (院人才项目) 2017.01-2020.12
- 中国科学院信息工程研究所青年之星 (所人才项目) 2014.01-2016.12

教学 (中国科学院大学)

- 2017 春季, 2018 春季、秋季 理论密码学 @ 中国科学院大学网络空间安全学院
- 2018 夏季 高级密码组件及其应用 @ 中国科学院大学网络空间安全学院

学术服务

- 审稿人: ASIACRYPT (2012, 2013, 2016, 2017), PKC (2018, 2019)
- 程序委员会委员: INSCRYPT 2014, Provsec 2016, CANS 2017, INSCRYPT 2018
- 中国密码学会青年工作委员会委员

奖励

- 2018 年密码创新奖二等奖 (个人奖)

CCF Rank CACR Rank

期刊论文 (部分)

1. **Yu Chen**, Jiang Zhang, Yi Deng, Jinyong Chang. KDM Security for IBE: Generic Constructions and Separations. *Information Sciences*. (CCF B)
2. **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)
3. **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)
4. **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. (CCF B)
5. **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)
6. 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)
7. **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 B)
8. **Yu Chen**, Zongyang Zhang, Dongdai Lin, Zhenfu Cao. Generalized (Identity-Based) Hash Proof System and Its Applications. *Security and Communication Networks*, online. A preliminary version of this paper appears in Provsec 2012. (CCF C)
9. **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)
10. 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. (CCF B)

会议论文 (部分)

1. **Yu Chen**, Yuyu Wang, Hong-Sheng Zhou. Leakage-Resilient Cryptography from Puncturable Primitives and Obfuscation. *ASIACRYPT 2018*. (CACR A)
2. **Yu Chen**, Baodong Qin, Haiyang Xue. Regularly Lossy Functions and Their Applications in Leakage-Resilient Cryptography. *CT-RSA 2018*. (CACR B)
3. Zheng Yang, **Yu Chen**, Song Luo. Two-message Key Exchange with Strong Security from Ideal Lattices. *CT-RSA 2018*. (CACR B)

4. Yi Deng, Xuyang Song, Jingyue Yu, **Yu Chen**. On the Security of Classic Protocols for Unique Witness Relations. *PKC 2018*. (CCF B)
5. Jingyue Yu, Yi Deng, **Yu Chen**. From Attack on Feige-Shamir to Construction of Oblivious Transfer. *INSCRYPT 2017*. (CACR C)
6. 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)
7. 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)
8. **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)
9. 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)
10. 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. (CACR A)
11. **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 B)
12. **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. (CCF C)
13. 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)
14. **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)
15. **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)
16. **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)
17. 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)
18. **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.
19. **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.

20. **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)
21. 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)
22. **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)
23. **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.
24. **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)