

Jiliang ZHANG
IEEE/CCF/CIE Senior Member

College of Semiconductors (College of Integrated Circuits), Hunan University, Changsha 410082, China.
zhangjiliang@hnu.edu.cn <https://hardwaresecurity.cn/>

Notarization: I have read the following and certify that this curriculum vitae is a current and accurate statement of my professional record.

Signature _____ Date _____

1. Personal Information

Current Position:

Professor in College of Integrated Circuits, Hunan University, Changsha, China
Vice Dean of the College of Integrated Circuits, Hunan University
Director of Chip Security Institute of Hunan University, China
Chair Professor of Anhui University, China
Secretary-General of CCF Fault-Tolerant Computing Professional Committee

a. Educational Background

- Apr. 2015 Ph.D. Computer Science and Technology, Hunan University, China.
Dissertation: "Security and Trust for FPGA-based Systems". (**Outstanding Doctoral dissertation of Hunan University**)
- Jul. 2009 B.E. Chemical Engineering and Technology, Shandong University of Science and Technology, Qingdao, China.

b. Honors and Awards

- 2022 Recipient of the Second Natural Science Award of Hunan Province.
- 2022 Recipient of the CCF Distinguished lecturer.
- 2022 Recipient of the World's Top 2% Scientists, Stanford University, 2022, ranked globally 16th in the computer hardware and architecture.
- 2022 Recipient of the Featured Paper of IEEE Transactions on Computers.
- 2022 Recipient of the Best Paper Award of Tsinghua Science and Technology, 202202
- 2021 Recipient of the World's Top 2% Scientists (Stanford University), 2021
- 2021 Recipient of the Most Beautiful Scientists of the Institute of Electronics of Hunan Province.
- 2021 Recipient of the Excellent Young Scientists Fund Program of National Natural Science Fund.

2021	Recipient of the Science and technology innovation leader of Hunan Province.
2021	Recipient of the CCF Integrated Circuit Early Career Award.
2020	Recipient of the World's Top 2% Scientists (Stanford University), 2020
2020	Recipient of the Yuelu Fellow of Hunan University.
2020	Recipient of the Hunan Natural Science Fund for Distinguished Young Scholars.
2020	Recipient of the Distinguished Faculty Award of Hunan University.
2020	Recipient of the Distinguished New Faculty Award of Hunan University.
2018	Recipient of the Hu-Xiang Youth Talent, Hunan Province.

Students' Honors and Awards

Nov. 2021	National Scholarship for Doctoral Students. (Chaoqun Shen)
Jul. 2021	Scientific Research and Innovation Project of Hunan Province. (Chaoqun Shen)
July 2020	CCF DAC Outstanding Volunteer (Chaoqun Shen)
Aug. 2020	The Third Prize, National College Student Information Security Contest, Beijing, China. (Lin Shi, Yibo Qu, Xiao Wang and Weilong Wang)
Oct. 2019	National Scholarship for Postgraduates, China. (Cheng Li)
Jul. 2019	Full Scholarship, CUHK Exchange Program. (Lu Wan)
Aug. 2019	The Second Prize, National College Student Information Security Contest, Nanjing, China. (Chengjie Liu, Lin Shi, Yuqi Niu and Yayi Wang)
May. 2019	The First Prize & The Baidu Brain Special Award, HackBJ AI Hackthon, Beijing, China. (Yehao Kong and Xiaoxiong Jiang)
Nov. 2018	The Second Prize, "HackFun" Hackthon of Central China. (Yehao Kong and Xiaoxiong Jiang)
Jun. 2018	National-level Student Innovation Training Program. (Zhiwei Huang)
May 2018	Outstanding Paper Award (The First Prize), 11th excellent graduate innovative forum, Hunan province. (Haihan Su)
May 2018	Outstanding Paper Award (The Second Prize), 11th excellent graduate innovative forum, Hunan province. (Xiaoxiong Jiang)
Apr. 2017	The Second Prize, "Zhongtian steel" College Student Information Security, Contest, Northeastern University, China. (Binhang Qi)
Apr. 2017	The Third Prize, "Zhongtian steel" College Student Information Security Contest, Northeastern University, China. (Binhang Qi)
May. 2016	National-level Student Innovation Training Program. (Yuanjing Zhang)

c. Professional Experience

Dec. 2020-Present	Hunan University, Professor
May. 2017-Dec. 2020	Hunan University, Associate Professor

May. 2015-Apr.2017	Northeastern University, Associate Professor (Promotion date 2015/05)
Sept. 2013-Sept.2014	Department of Electrical and Computer Engineering, University of Maryland, College Park, Research Scholar
Aug. 2012-Sept.2012	Research Institute of Information Technology, Tsinghua University, Beijing China, Visiting Research
Sept. 2010-Jun. 2011	Department of Computer Science and Technology, Tsinghua University, Beijing China, Visiting Research

2. Research, Scholarly, and Creative Activities

Research Interests

Hardware Security: Physical unclonable functions; True Random Number Generator; Hardware obfuscation; Hardware IP protection (watermarking, metering); FPGA Security; Hardware Trojan attacks and detection techniques; Cryptographic accelerator; CPU Security; Hardware techniques to facilitate software and/or system security; Applications of hardware security to secure system and so on.

New computing architectures: In-memory Computing; Brain-inspired Computing

Summary:

Google Scholar Citations: 2433, H-index of the first/corresponding author papers: 27.

a. Articles in Refereed Journals

- A.1 **Jiliang Zhang***, Chaoqun Shen, and Gang Qu, “*Mex+Synch*: Software Cache Write Covert Channels Exploiting Mutual Exclusion and Synchronization Mechanisms”, *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2023. DOI: 10.1109/TCAD.2023.3291669
- A.2 Qinghui Hong, Haotian Fu, Yiyang Liu, and **Jiliang Zhang***, “In-Memory Computing Circuit Implementation of Complex-Valued Hopfield Neural Network for Efficient Portrait Restoration”, *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2023, DOI 10.1109/TCAD.2023.3242858
- A.3 Yuan Zhang, **Jiliang Zhang***, “A High Throughput STR-based TRNG by Jitter Precise Quantization Superposing,” *ACM Transactions on Design Automation of Electronic Systems*, 2023. <https://doi.org/10.1145/3606373>
- A.4 Pingdan Xiao, Qinghui Hong*, Jingru Sun, Sichun Du, and **Jiliang Zhang***, “Design and Application of Programmable Analog Circuit for Solving Lyapunov Matrix Equation Based on Memristors”, *IEEE Transactions on Industrial Electronics*, 2023.
- A.5 Sichun Du, Jun Li, Chen Sun, Pingdan Xiao, Qinghui Hong*, **Jiliang Zhang***, “Analog In-memory Circuit Design of Polynomial Multiplication for Lattice Cipher Acceleration”, *ACM Transactions on Embedded Computing Systems*, 2023. <https://doi.org/10.1145/3605891>
- A.6 Pingdan Xiao, Qinghui Hong*, Jingru Sun, Member, IEEE, Sichun Du, and **Jiliang Zhang***, “Design and Application of Programmable Analog Circuit for Solving Lyapunov Matrix Equation Based on Memristors”, *IEEE Transactions on Industrial Electronics*, 2023.
- A.7 Qinghui Hong, Shen Man, Chunhua Wang, Jingru Sun, Sichun Du, **Jiliang Zhang***, “Programmable In-Memory Computing Circuit for Solving Combinatorial Matrix Operation in

- One Step”, *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2023, DOI: 10.1109/TCSI.2023.3263217.
- A.8 Dan Tang, Siyuan Wang, Boru Liu, Wenqiang Jin, **Jiliang Zhang***, “GASF-IPP: Detection and Mitigation of LDoS Attack in SDN,” *IEEE Transactions on Services Computing*, 2023, DOI: 10.1109/TSC.2023.3266757.
- A.9 **Jiliang Zhang***, Shuang Peng, Yansong Gao, Zhi Zhang, Qinghui, “APMSA: Adversarial Perturbation against Model Stealing Attacks”, *IEEE Transactions on Information Forensics & Security*, vol. 18, pp.1667-1679, 2023.
- A.10 Qinghui Hong, Bang He, Zedi Zhang, Pingdan Xiao, Sichun Du, **Jiliang Zhang***, “Circuit Design and Application of Discrete Cosine Transform based on Memristor”, *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, 2023, DOI: 10.1109/JETCAS.2023.3243569.
- A.11 Aibin Yan, Runqi Liu, Jie Cui, Tianming Ni, Patrick Girard, Xiaoqing Wen, and **Jiliang Zhang*** “Designs of BCD Adder Based on Excess-3 Code in Quantum-dot Cellular Automata”, *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2023, vol. 70, no.6, pp..
- A.12 Dan Tang, Chenjun Gao, Wei Liang, **Jiliang Zhang***, Keqin Li, “FTMaster: A Detection and Mitigation System of Low-rate Flow Table Overflow Attacks via SDN”, *IEEE Transactions on Network and Service Management*, 2023, DOI: 10.1109/TNSM.2023.3270339.
- A.13 Hua Ma, Huming Qiu, Yansong Gao, Zhi Zhang, Alsharif Abuadbba, Minhui Xue, Anmin Fu, **Jiliang Zhang**, Said F. Al-Sarawi, Derek Abbott, “Quantization Backdoors to Deep Learning Commercial Frameworks”, *IEEE Transactions on Dependable and Secure Computing*, 2023, DOI: 10.1109/TDSC.2023.3271956
- A.14 Dan Tang, Zhiqing Zheng, Keqin Li, Chao Yin, Wei Liang and **Jiliang Zhang***, “FTOP: An Efficient Flow Table Overflow Preventing System for switches in SDN”, *IEEE Transactions on Network and Service Management*, 2023.
- A.15 肖平旦, 洪庆辉, 杜四春, 孙辰, 黎俊, 张吉良, 基于忆阻器的可编程矩阵行列式求解电路设计及应用, *中国科学: 信息科学*, 2023, 53(5): 1008-1025
- A.16 He Li, Yongming Tang and, **Jiliang Zhang***, “FPGA Accelerated Post-Quantum Cryptography”, *IEEE Transactions on Nanotechnology*, vol.21, pp. 685-691, Oct. 2022.
- A.17 Yupeng Hu, Linjun Wu, Zhuojun Chen, Xiaolin Xu, Keqin Li, **Jiliang Zhang***, “STT-MRAM-based Reliable Weak PUF”, *IEEE Transactions on Computers*, 2022. vol.71, no.7, pp. 1564-1574
- A.18 **Jiliang Zhang***, Chaoqun Shen, Haihan Su, Md Tanvir Arafin, Gang Qu, “Voltage Over-scaling-based Lightweight Authentication for IoT Security”, *IEEE Transactions on Computers*, vol.71, no.2, pp. 323-336, Feb. 2022. (Featured Paper, Highly Cited Paper)
- A.19 Zhuojun Chen, Wenshang Lee, Qinghui Hong, Chongyan Gu, Zhenyu Guan, Lin Ding, and **Jiliang Zhang***, “A Lightweight and Machine-Learning-resistant PUF using Obfuscation Feedback Shift Register”, *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 69, no. 11, pp. 4543-4547, Nov. 2022.
- A.20 Y Hu, W Kuang, Z Qin, K Li, **Jiliang Zhang***, Y Gao, W Li, K Li, “Artificial Intelligence Security: Threats and Countermeasures”, *ACM Computing Surveys*, vol. 55, no. 1, Article 20, Jan. 2023.
- A.21 Wenhao Wang, Guangyu Hu, Xiaolin Xu, **Jiliang Zhang***, “CRAlert: Hardware-assisted Code Reuse Attack Detection”, *IEEE Transactions on Circuits and Systems—II: Express Briefs*, vol. 69, no. 3, pp. 1607-1611, March 2022.

- A.22 **Jiliang Zhang***, Chaoqun Shen, Zhiyang Guo, Qiang Wu, Wanli Chang, “CT PUF: Configurable Tristate PUF against Machine Learning Attacks for IoT Security”, *IEEE Internet of Things Journal*, vol. 9, no. 16, pp. 14452-14462, Jun. 2022.
- A.23 Hanpu Zhou , Zhuoying Fei , Qinghui Hong , Jingru Sun , Sichun Du , Tao Li , **Jiliang Zhang**, “Bionic Dual-loop Emotional Learning Circuit and Its Application In Radiation Early Warning Monitor”, *IEEE Transactions on Cognitive and Developmental Systems*, 2022.
- A.24 Hegan Chen, Qinghui Hong, Zhongrui Wang, Chunhua Wang, Xiangxiang Zeng and **Jiliang Zhang**, “Memristive Circuit Implementation of Caenorhabditis Elegans Mechanism for Neuromorphic Computing,” *IEEE Transactions on Neural Networks and Learning Systems*, 2022.
- A.25 He Li, Ameer Abdelhadi, Runbin Shi, **Jiliang Zhang***, Qiang Liu*, “Adversarial Hardware with Functional and Topological Camouflage”, *IEEE Transactions on Circuits and Systems—II: Express Briefs*, May 2021, vol. 68, no. 5, pp. 1685-1689.
- A.26 **Jiliang Zhang***, Chaoqun Shen, “Set-based Obfuscation for Strong PUFs against Machine Learning Attacks”, *IEEE Transactions on Circuits and Systems I: Regular Papers*, Jan. 2021, vol. 68, no. 1, pp.288-300. (Highly Cited Paper)
- A.27 Junye Shi, Yang Lu, **Jiliang Zhang***, “Approximation Attacks on Strong PUFs”, *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2020, vol.39, no.10, pp. 2138-2151 (Highly Cited Paper)
- A.28 **Jiliang Zhang***, Gang Qu, “Physical Unclonable Function-based Key-Sharing via Machine Learning for IoT Security”, *IEEE Transactions on Industrial Electronics*, 2020, vol. 67, no. 8, pp. 7025-7033. (Hot Paper)
- A.29 **Jiliang Zhang***, Chen. Li, “Adversarial Examples: Opportunities and Challenges,” *IEEE Transactions on Neural Networks and Learning Systems*, 2020, vol.31, no.7, pp. 2578-2593.
- A.30 **Jiliang Zhang***, B. Qi, Z. Qin, G. Qu, “HCIC: Hardware-assisted Control-flow Integrity Checking”, *IEEE Internet of Things Journal*, 2019, vol. 6, no. 1, pp. 458-471.
- A.31 **Jiliang Zhang***, Gang Qu, “Recent Attacks and Defenses on FPGA-based Systems”, *ACM Transactions on Reconfigurable Technology and Systems*, 2019, Article No.14, DOI: 10.1145/3340557.
- A.32 A. Yan, K. Yang, Z. Huang, **Jiliang Zhang***, et al., “A Double-Node-Upset Self-Recoverable Latch Design for High Performance and Low Power Application”, *IEEE Transactions on Circuits and Systems--II: Express Briefs*, vol. 66, no. 2, pp. 287-291, Feb. 2019.
- A.33 Pengfei Qiu, Yongqiang Lv, **Jiliang Zhang***, et al., “Control Flow Integrity based on Lightweight Encryption Architecture”, *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 37, no. 7, pp. 1358-1369, July 2018
- A.34 **Jiliang Zhang***, X. Tan, Y. Zhang, et al., “Frequency Offset-based Ring Oscillator Physical Unclonable Function”, *IEEE Transactions on Multi-Scale Computing Systems*, vol. 4, no. 4, pp. 711-721, Oct.-Dec. 2018.
- A.35 **Jiliang Zhang***, Lele Liu, “Publicly Verifiable Watermarking for Intellectual Property Protection in FPGA Design”, *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 4, pp. 1520-1527, April, 2017
- A.36 **Jiliang Zhang***, Gang Qu, “A Rebuttal to Comments on A PUF-FSM Binding Scheme for FPGA IP Protection and Pay-per-Device Licensing”, *IEEE Transactions on Information Forensics and Security (TIFS)*, 2016, vol.11, no.11, pp. 2626 - 2627.

- A.37 **Jiliang Zhang***, “A Practical Logic Obfuscation Technique for Hardware Security”, *IEEE Transactions on Very Large Scale Integration Systems (TVLSI)*, 2016, vol. 24, no. 3, pp. 1193-1197.
- A.38 **Jiliang Zhang***, Yaping Lin, Yongqiang Lyu, Gang Qu, “A PUF-FSM Binding Scheme for FPGA IP Protection and Pay-per-Device Licensing”, *IEEE Transactions on Information Forensics and Security (TIFS)*, 2015, vol.10, no.6, pp. 1137-1150.
- A.39 **Jiliang Zhang***, Yaping Lin, Gang Qu, “Reconfigurable Binding against FPGA Replay Attacks”, *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, vol. 20, no.2, February 2015, pp.1-20.
- A.40 **Jiliang Zhang**, X. Tan, X. Wang, A. Yan, Z. Qin, “T2FA: Transparent Two-Factor Authentication”, *IEEE Access*, 2018, vol.6, pp.32677-32686.
- A.41 X. Tan, **Jiliang Zhang***, Y. Zhang, Z. Qin, Y. Ding, and X. Wang, “A PUF-based and Cloud-assisted Lightweight Authentication Mechanism for Multi-hop Body Area Network”, *Tsinghua Science and Technology*, 2021, 26(1), pp.36-47. (Best Paper Award)
- A.42 Yaping Lin, Xinbo Liu, He Li, **Jiliang Zhang**, “A Novel Method for Malware Detection on ML-based Visualization Technique”, *Computers & Security*, vol. 89, Feb. 2020.
- A.43 **Jiliang Zhang***, W. Wang, X. Wang, Z. Xia, “Enhancing Security of FPGA-based Systems with Combinational Logic Binding”, *Journal of Computer Science and Technology (JCST)*, 2017, vol.32, no.2, pp.329-339.
- A.44 **Jiliang Zhang**, Qiang Wu, Yipeng Ding, et al., “Techniques for Design and Implementation of an FPGA-specific Physical Unclonable Function”, *Journal of Computer Science and Technology (JCST)*, 31(1): 124–136, Jan. 2016.
- A.45 He Li, Qiang Liu, **Jiliang Zhang***, “A survey of Hardware Trojan Threat and Defense”, *Integration, the VLSI Journal*, vol. 55, pp.426-437, Sep. 2016.
- A.46 Qian Wang, Liji Wu, An WANG, **Jiliang Zhang**. “A New Zero Value Attack Combined Fault Sensitivity Analysis on Masked AES”, *Microprocessors and Microsystems*, vol. 45, Part B, pp.355-362, Sep. 2016.
- A.47 Dongqi Wang, Dongming Chen, Ben Ma, Lisheng Xu, **Jiliang Zhang**, “A High Capacity Spatial Domain Data Hiding Scheme for Medical Images”, *Journal of Signal Processing Systems*, DOI: 10.1007/s11265-016-1169-7 .
- A.48 Yipeng Ding*, Jingtian Tang, Xuemei Xu, **Jiliang Zhang**, “Application of Linear Predictive Coding for Doppler Through-Wall Radar Target Tracking”, *IEEE Geoscience and Remote Sensing Letters*. 2015, 12(6): 1317-1321.
- A.49 Yipeng Ding*, Jingtian Tang, Xuemei Xu, **Jiliang Zhang**, “Echo Interference Suppression Approach for Doppler Through-Wall Radar”, *IEEE Sensors Journal*, 2015, 15(6): 3395-3402.
- A.50 **Jiliang Zhang**, Gang Qu*, Yongqiang Lyu, Qiang Zhou, “A Survey on Silicon PUFs and Recent Advances in Ring Oscillator PUFs”, *Journal of Computer Science and Technology (JCST)*, 2014, vol. 29, no. 4, pp. 664-678.
- A.51 **Jiliang Zhang***, Yaping Lin, Qiang Wu, Wenjie Che, “Watermarking FPGA Bitfile for Intellectual Property Protection”, *Radioengineering*, 2012, vol.21, no 2, pp.764-771.

- A.52 **Jiliang Zhang***, Yaping Lin, Wenjie Che, et al., “Efficient verification of IP watermarks in FPGA designs through lookup table content extracting”, *IEICE Electronics Express (Elex)*, 2012, vol. 9, no. 22, pp. 1735-1741.
- A.53 **Jiliang Zhang***, Yongqiang Lyu, Qiang Zhou, Qiang Wu, Yaping Lin, and Kang Zhao, “TimFastPlace: Critical-Path based Timing Driven FastPlace”, *IEICE Electronics Express (Elex)*, 2012, vol.9, no16, pp.1310-1315.
- A.54 **Jiliang Zhang***, Yaping Lin, Yongqiang Lyu, Qiang Zhou, Qiang Wu, “A delay-driven fast placement algorithm based on sensitivity”. *Chinese Journal of Electronics*, 2012, vol.40, no. 12, pp. 2410-2414.
- A.55 **Jiliang Zhang***, Qiang Wu, Jiani Chen, “Research on Design Method of Dynamic Partial Reconfigurable System”. *Journal of Software Engineering*, 2012, vol.6, no 2, pp.21-30.
- A.56 **Jiliang Zhang**, Yaping Lin, Yongqiang Lyu, Xiangqi Wang, “Chaos-based Public Verifiable FPGA Intellectual Property Kernel Watermark Detection Scheme”, *Chinese Science: Information Science*, vol.43, no.9, pp. 1096-1110.

b. Articles in Conference, Symposium, and Workshop Proceedings

- B.1 Lin Ding, Song Bian, **Jiliang Zhang***, LIMA-LPN: MRAM-based Logic-in-memory Accelerator for Efficient Learning Parity with Noise Cryptography, *In Proceedings of the 60th IEEE/ACM Design Automation Conference (DAC'23)*, San Francisco, CA, July 2023. (CCF A)
- B.2 Chaoqun Shen, **Jiliang Zhang***, Gang Qu, MES-Attacks: Software-Controlled Covert Channels based on Mutual Exclusion and Synchronization, *In Proceedings of the 60th IEEE/ACM Design Automation Conference (DAC'23)*, San Francisco, CA, July 2023. (CCF A)
- B.3 Zhaojun Lu, Houjia Qidiao, Qidong Chen, Zhenglin Liu, and **Jiliang Zhang***, An Ultra High-Throughput and Energy-Efficient TRNG Exploiting Four FPGA-Compatible Ring Oscillators and One Multiphase Sampler, *In Proceedings of the 60th IEEE/ACM Design Automation Conference (DAC'23)*, San Francisco, CA, July 2023. (CCF A)
- B.4 Jinhua Cui, Yiyun Yin, Congcong Chen and **Jiliang Zhang***, SPOILER-ALERT: Detecting SPOILER Attack Using Cuckoo Filter, *In Proceedings of the 26th Design, Automation and Test in Europe Conference (DATE'23)*, Antwerp, Belgium, April 2023.
- B.5 **Jiliang Zhang***, Lin Ding, Zhuojun Chen, Wenshang Li and Gang Qu, DA PUF: Dual-State Analog PUF, *In Proceedings of the 59th IEEE/ACM Design Automation Conference (DAC'22)*, San Francisco, CA, July 2022, pp. 73-78.
- B.6 Congcong Chen, Chaoqun Shen, **Jiliang Zhang***, “Lightweight and Secure Branch Predictors against Spectre Attacks”, *In Proceedings of the 27th Asia and South Pacific Design Automation Conference (ASPDAC)*, January 17–20, 2022, Virtual Conference, pp. 20-30. (Invited Paper)
- B.7 He Li, Yaru Pang, **Jiliang Zhang***, “Security Enhancements for Approximate Machine Learning”, in *Proceedings of the 31st edition of the ACM Great Lakes Symposium on VLSI (GLSVLSI)*, June 22--25, 2021, Virtual Event, USA, pp. 461-466. (Invited Paper)
- B.8 **Jiliang Zhang***, Junjie Hou, “Unpaired Image-to-Image Translation Network for Semantic-based Face Adversarial Examples Generation”, in *Proceedings of the 31st edition of the ACM Great Lakes Symposium on VLSI (GLSVLSI)*, June 22--25, 2021, Virtual Event, USA, pp. 449-454. (Invited Paper)
- B.9 Chaoqun Shen, Congcong Chen, **Jiliang Zhang***, “Cache Side-Channel Attacks and Countermeasures”, *In 26th Asia and South Pacific Design Automation Conference (ASPDAC)*,

- January 18–21, 2021, Tokyo, Japan, pp. 441-448. (Invited Paper)
- B.10 **Jiliang Zhang***, Chen Li, Jing Ye, Gang Qu, “Privacy Threats and Protection in Machine Learning”, *in the 30th edition of the ACM Great Lakes Symposium on VLSI (GLSVLSI)*, Beijing China, Sept. 2020, pp. 531-536. (Invited Paper)
- B.11 Qiang Wu, **Jiliang Zhang***, “CT PUF: Configurable Tristate PUF Against Machine Learning Attacks”, *In IEEE International Symposium on Circuits & Systems (ISCAS)*, Seville, Spain, May 17-20, 2020, pp. 531-536.
- B.12 Yehao Kong, **Jiliang Zhang***, “Adversarial Audio: A New Information Hiding Method”, *in the 21st Conference of the International Speech Communication Association (INTERSPEECH)*, Shanghai, Oct. 2020, pp. 1-5.
- B.13 **Jiliang Zhang**, Shuang Peng, Yupeng Hu, Fei Peng, Wei Hu, Jinmei Lai, Jing Ye, Xiangqi Wang*, “HRAE: Hardware-assisted Randomization against Adversarial Example Attacks”, *in the 29th IEEE Asian Test Symposium*, 2020, pp. 1-6. (Invited Paper)
- B.14 Wei Hu, Lingjuan Wu, Yu Tai, Jing Tan and **Jiliang Zhang**, “A Unified Formal Model for Proving Security and Reliability Properties”, *in the 29th IEEE Asian Test Symposium*, 2020, pp. 1-6.
- B.15 Yipei Yang, Jing Ye, Yuan Cao, **Jiliang Zhang**, Xiaowei Li, Huawei Li and Yu Hu, *Survey: Hardware Trojan Detection for Netlist*, *in the 29th IEEE Asian Test Symposium*, 2020, pp. 1-6.
- B.16 Xiaolin Xu, **Jiliang Zhang**, “Rethinking FPGA Security in the New Era of Artificial Intelligence”, *In the 21st International Symposium on Quality Electronic Design (ISQED)*, Santa Clara, California, USA, March 25-26, 2020, pp. 46-51. (Invited Paper)
- B.17 Qingli Guo, Jing Ye*, **Jiliang Zhang**, Yu Hu, Xiaowei Li, Huawei Li, “Prediction Stability: A New Metric for Quantitatively Evaluating DNN Outputs”, *in the 30th edition of the ACM Great Lakes Symposium on VLSI (GLSVLSI)*, Beijing China, Sept. 2020, pp. 537-542. (CCF C) (Invited Paper)
- B.18 Pengfei Qiu, Yongqiang Lyu, **Jiliang Zhang***, et al., “Physical Unclonable Functions-based Linear Encryption against Code Reuse Attacks”, *in 53rd Design Automation Conference (DAC)*, Austin, USA, June 5-9 2016, pp. 1-6.
- B.19 Xinbo Liu, **Jiliang Zhang***, et al., “ATMPA: Attacking Machine Learning-based Malware Visualization Detection Methods via Adversarial Examples”, *in IEEE/ACM International Symposium on Quality of Service (IWQoS)*, Phoenix, AZ, USA, June 24-25, 2019, pp. 1-10.
- B.20 Haihan Su, **Jiliang Zhang***, “Machine Learning Attacks on Voltage Over-scaling-based Lightweight Authentication”, *Asian Hardware Oriented Security and Trust Symposium (AsianHOST)*, Hongkong, China, 2018, pp. 50-55.
- B.21 Zihan Pang, **Jiliang Zhang***, Qiang Zhou, Shuqian Gong, et al. “Crossover Ring Oscillator PUF”, *in the 18th International Symposium on Quality Electronic Design (ISQED)*, 2017, pp. 237-243. (Best Paper Nomination)
- B.22 **Jiliang Zhang***, “Combinational Logic Binding for FPGA System Security”, *In 15th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Tianjin, China, August 23-26, 2016, pp. 216-223.
- B.23 **Jiliang Zhang***, Gang Qu, “A Survey on Security and Trust of FPGA-based Systems”, *in 13th International Conference on Field Programmable Technology (FPT’14)*, 2014, pp.147-152.
- B.24 Mingze Gao, Khai Lai, **Jiliang Zhang**, Gang Qu, Aijiao Cui, Qiang Zhou, “Reliable and Anti-Cloning PUFs Based on Configurable Ring Oscillators”, *in 14th International Conference on*

Computer-Aided Design and Computer Graphics, 2015, pp.194-201,

- B.25 He Li, Qiang Liu, **Jiliang Zhang***, Yongqiang Lyu, “A survey of Hardware Trojan Detection, Diagnosis and Prevention”, *in 14th International Conference on Computer-Aided Design and Computer Graphics*, 2015, pp.173-179.
- B.26 Bing Tang, Yaping Lin, **Jiliang Zhang**, “Improving the Reliability of RO PUF using Frequency Offset”, *in 13th International Conference on Field Programmable Technology (FPT’14)*, 2014, pp.338-341.
- B.27 **Jiliang Zhang**, Yaping Lin, Yongqiang Lyu, Gang Qu, Cheung, R.C.C., Wenjie Che, Qiang Zhou, Jinian Bian, “FPGA IP Protection by Binding Finite State Machine to Physical Unclonable Functions”, *in 23rd IEEE International Conference on Field Programmable Logic and Applications (FPL’13)*, Porto, Portugal, Sept. 2013, pp.1-4.
- B.28 **Jiliang Zhang***, Yaping Lin, Yongqiang Lyu, Cheung, R.C.C., Wenjie Che, Qiang Zhou, Jinian Bian, “Binding Hardware IPs to Specific FPGA Device via Inter-twining the PUF Response with the FSM of Sequential Circuits”, *in 21st IEEE International Symposium on Field-Programmable Custom Computing Machines (FCCM’13)*, Seattle, USA, 2013, Poster, pp. 227-227.
- B.29 **Jiliang Zhang***, Qiang Wu, Yongqiang Lyu, Yaping Lin, Qiang Zhou, Yici Cai, Gang Qu, “Design and Implementation of a Delay-based PUF for FPGA IP Protection”, *in 13th IEEE International Conference on Computer-Aided Design and Computer Graphics (CAD/Graphics’13)*, HK, 2013, pp. 107-114.

c. Invited Talks and Professional Presentations

- C.1 **(Invited Talks)** “Security base in the Era of Intelligent Internet of Everything: Lightweight Security Chip Design”, Hefei University of Technology, 22 May, 2023
- C.2 **(Invited Talks)** “CPU Security”, Anhui University, 21 May, 2023
- C.3 **(Invited Talks)** “Security base in the Era of Intelligent Internet of Everything: Lightweight Security Chip Design”, Hunan University of Technology and Business, 18 May, 2023
- C.4 **(Invited Talks)** “CPU Security”, Northwestern Polytechnical University, 14 May, 2023
- C.5 **(Invited Talks)** “Security base in the Era of Intelligent Internet of Everything: Lightweight Security Chip Design”, Zhejiang Hikstor Technology Co.Ltd, 24 April, 2023
- C.6 **(Invited Talks)** “Hardware Security Primitives”, Zhejiang University, 23 April, 2023
- C.7 **(Invited Talks)** “Microarchitecture Security for Processors”, Ningbo University, 27 March, 2023.
- C.8 **(Invited Talks)** “Hardware Security for Integrated Circuits”, Wenzhou University, 26 March, 2023.
- C.9 **(Invited Talks)** “Information Security Chips”, Roundtable Forum of the Annual Conference of Circuits and Systems Branch, Chinese Institute of Electronics, Wenzhou, 25 March, 2023.
- C.10 **(Invited Talks)** “A True Random Number Generator with High Throughput and High Energy Efficiency”, Beihang University, 19 March, 2023
- C.11 **(Invited Talks)** “Security base in the Era of Intelligent Internet of Everything: Lightweight Security Chip Design”, Nankai University, 28 Nov., 2022.

- C.12 **(Invited Talks)** “Security base in the Era of Intelligent Internet of Everything: Lightweight Security Chip Design”, Taishan Science and Technology Forum, 26 Nov., 2022.
- C.13 **(Invited Talks)** “Security base in the Era of Intelligent Internet of Everything: Lightweight Security Chip Design”, Frontier Forum of Information Science, Guangzhou University & Hong Kong University of Science and Technology (Guangzhou), 11 Nov., 2022.
- C.14 **(Invited Talks)** “Hardware Security for Integrated Circuits”, Annual Cyberspace Security Meeting of Hunan, Xiangyang, 23 Jul., 2022
- C.15 **(Invited Talks)** “Security base in the Era of Intelligent Internet of Everything: Lightweight Security Chip Design”, Wenzhou University, 18 Jul., 2022.
- C.16 **(Invited Talks)** “IC Design and New Computing Architectures”, Hunan University of Technology and Business, 18 Jul., 2022 (online).
- C.17 **(Invited Talks)** “Security base in the Era of Intelligent Internet of Everything: Lightweight Security Chip Design”, Huazhong University of Science and Technology, 23 Jun., 2022.
- C.18 **(Invited Talks)** “Security base in the Era of Intelligent Internet of Everything: Lightweight Security Chip Design”, Hubei University of Technology, 24 Jun., 2022.
- C.19 **(Invited Talks)** “Hardware Security for Integrated Circuits”, Huazhong Agricultural University, 24 Jun., 2022.
- C.20 **(Invited Talks)** “Highly Reliable and Dual-State Analog PUF”, Hunan University of Science and Technology, 10 Jun., 2022.
- C.21 **(Invited Talks)** “Highly Reliable and Dual-State Analog PUF”, Changsha University of Science & Technology, 29 May, 2022.
- C.22 **(Keynote)** “PUF Design and Applications”, CACR Conference on Cryptography Chips (CryptoIC), Harbin, 28 Dec., 2021.
- C.23 **(Invited Talks)** “Opportunities and Challenges Faced by PUF Chip Technology”, China Computer Federation CNC “Trusted Chip Design and Testing: from Internet of Things Chips to Automotive Electronics” Forum, Shenzhen, 18 Dec., 2021.
- C.24 **(Invited Talks)** “Design of Physical Unclonable Security Chip”, “Password and Information Security” Frontier Technology Seminar of China University of Geosciences, 13 Nov., 2021.
- C.25 **(Invited Talks)** “PUF Design and Applications”, The 58th Research Institute of CETC, Wuxi, 9 July, 2021. Host: Zongguang Yu.
- C.26 **(Invited Talks)** “PUF Design and Applications”, IC Test Summit Forum of Chinese Institute of Metrology, 18 May 2021.
- C.27 **(Invited Talks)** “PUF Design and Applications”, CCF Advanced Computer Architecture (ACA2020), Computer System Security and Future Architecture Forum, 15 Aug., 2020.
- C.28 **(Specially Invited Guest)** “Independent, Controllable and Hardware Security”, CCF Young Elite Forum, Panel: In the era of ‘new infrastructure’, where is the road of domestic controllable and controllable information system, 7 June, 2020.
- C.29 **(Invited Talks)** “PUF Design and Applications”, Beihang University (virtual), 30 Sept., 2020, Host: Zhenyu Guan.
- C.30 **(Invited Talks)** “Turn the Dust into Glory: Design of Physical Unclonable Functions”, Southeast University, Nanjing, 10 Aug., 2019, Host: Weiwei Shan.

- C.31 **(Keynote)** “Hardware and Hardware-assisted Security”, CACR Conference on Cryptography Chips (CryptoIC), Nanjing, 2019.
- C.32 **(Keynote)** “Hardware and Hardware-assisted Security”, International Software and Hardware Design and Implementation Forum, Guilin, 2019.
- C.33 **(Invited Talks)** “Hardware and Hardware-assisted Security”, Shenzhen University, Shenzhen, 29 July, 2019, Host: Bin Li.
- C.34 **(Keynote)** “Hardware-assisted Security”, The Third Hardware Security Forum of China, Harbin, Aug. 2018.
- C.35 **(Invited Talks)** “Hardware-assisted Control-flow Integrity against Code-reuse Attacks”, State Key Laboratory of Computer Architecture, ICT, CAS, Beijing, Jul. 2018, Host: Jing Ye.
- C.36 **(Keynote)** “PUF and Applications”, The 5th Hardware Security Forum of China, Nantong, Aug. 24, 2016.
- C.37 **(Specially Invited Guest)** “Security for FPGA Systems”, Internet Conference of China (ICoC), TOP Conference/Journal paper Panel, Aug. 28, 2015.
- C.38 **(Invited Talks)** “Physical Unclonable Functions and Applications”, Huawei Technologies Co Ltd, Shenzhen, Jan. 2015, Host: Yuliang Zhou.
- C.39 **(Invited Talks)** “Physical Unclonable Functions and Applications”, Hardware Security workshop in China, Shenzhen, Jan. 2015.

d. Contracts and Grants

- D.1 Key Project of the National ** Foundation Strengthening Plan, Grant No. 2022-JCJQ-JJ-0406, “*** Chip Design”, 01/2023-12/2025, 3 million RMB, PI.
- D.2 Key Program of National Natural Science Foundation of China, “Physical Unclonable Security Chip Design and Applications”, Grant No. U20A20202, 01/2021~12/2024, 3.11 million RMB, PI.
- D.3 Excellent Young Scientists Fund of National Natural Science Foundation of China, “Hardware Security for Integrated Circuits”, Grant No. 62122023, 01/2022~12/2024, 2 million RMB, PI.
- D.4 Hunan Science and Technology Innovation Leading Talents Project, Grant No. 2021RC4019, 01/2022~12/2024, 1 million RMB, PI.
- D.5 Key R&D plan of the Ministry of Science and Technology, “Key Technologies and Application Verification of Component-based Elastic Integrated Navigation and Control”, Sub-project Leader, Grant No.2022YFB3903800, 01/2023-12/2025, 1.09 million RMB.
- D.6 “Hardware-assisted System Security”, Hunan Natural Science Foundation for Distinguished Young Scholars, Grant No. 2020JJ2010, 01/2020~12/2022, 0.5 million RMB, PI
- D.7 “Research and Development of Independent and Controllable Physical Unclonable Chip”, Key Research and Development Program of Hunan Province, China. Principal Investigator, Grant No. 2019GK2082, 10/2019~10/2021, 1 million RMB, PI
- D.8 Huawei Technologies Co., Ltd., “Research on the Reliability Technology of Software-based System Redundancy Instances”, 02/2022-08/2023, 1.03 million RMB.
- D.9 National Natural Science Foundation of China, “Hardware-assisted techniques against code reuse attacks”, Principal Investigator, Grant No. 61874042, 01/2019~12/2022, 0.63 million RMB, PI.

- D.10 National Natural Science Foundation of China, “Research on PUF and Obfuscation-based Active Defense Techniques for FPGA System Security”, Grant No. 61602107, 01/2017~12/2019, 0.21 million RMB, PI.
- D.11 The Hu-Xiang Youth Talent Program, Grant No. 2018RS3041, Grant No. 2018RS3041, 10/2018~10/2021, 0.5 million RMB, PI.
- D.12 Funded by Chinese National Key Laboratory of Science and Technology on Information System Security, “***bypass and verification”, 01/2019~12/2020, 0.3 million RMB, PI.
- D.13 CCF-IFAA Research Fund, Principal Investigator, “PUF and Voiceprint-based Transparent Two-Factor Authentication”, 03/2018~03/2019, 0.1 million RMB, PI.
- D.14 Natural Science Foundation of Fujian Province, “AI Security and Privacy Protection”, Grant No. 2021J01544, 01/2022~12/2025, 50 thousand RMB, PI.
- D.15 Natural Science Foundation of Hunan Province, “Intellectual Property Protection for Programmable Chips”, Grant No. 2018JJ3072, 01/2018~12/2020, 50 thousand RMB, PI.
- D.16 An enterprise project in Shenzhen, “Feasibility Analysis of Physical Unclonable Chip Technology in Blockchain”, 04/2021-07/2021, 0.3 million RMB, PI.

e. Patents

- E.1 **Jiliang Zhang**, Zhuojun Chen, Wenshang Li, Zhenyu Guan. “A Dual-state Physical Unclonable Function Circuit”. Patent application number: ZL 2021106580636
- E.2 **Jiliang Zhang**, Zihao Luo, “Defense Method and Deep Learning Model for Adversarial Attacks”, Patent application number: ZL202110411299X
- E.3 **Jiliang Zhang**, Junjie Hou. “Physical Unclonable Functions-based Lightweight Key Sharing Method”. Patent application number: ZL201910451161.5
- E.4 **Jiliang Zhang**. “Dynamic Multi-key obfuscation for PUF Structure and Authentication”. Patent application number: ZL201811052708.6
- E.5 **Jiliang Zhang**, Binhang Qi, Xiangqi Wang. “Hardware-assisted Defense System and Method against Code Reuse Attack”. Patent application number: ZL201710823354.3
- E.6 **Jiliang Zhang**, Yuanjing Zhang, Xiangqi Wang. “A Highly Reliable Physical Unclonable Function and Response Generation Method”. Patent application number: ZL201710718128.5
- E.7 **Jiliang Zhang**, Rui Jin. “Defense System and Method against Code Reuse Attacks”. Patent authorization number. ZL201610388347.7, Patent authorization time: 2018.10.23
- E.8 **Jiliang Zhang**, Yuanjing Zhang, Yong Ding, Weizhe Zhang. “Circuit, Control Method and Chip of Three-state Physical Unclonable Functions”. Patent application number: 202010094835.3
- E.9 **Jiliang Zhang**, Haihan Su, Weizhe Zhang, Yong Ding. “Authentication Device, Server, Authentication System and Authentication Method Based on Confusion Incentive”. Patent application number: 202010146250.1
- E.10 Yupeng Hu, Linjun Wu, **Jiliang Zhang**, Yun Huang, Jing Huang. “Magnetic random access memory and reconfigurable PUF method based on STT MARM”. Patent application number: 201910938265.9
- E.11 Jixin Zhang, Zheng Qin, Xiaofeng Huang, Yupeng Hu, **Jiliang Zhang**, Zibo Jiang. “An Active Safety Incremental Data Training Method”

f. Conference Chair/PC/TPC Member/Editor/Reviewer**Conference Chair/Editor**

- F.1 Program Chair, IEEE International Test Conference in Asia (ITC-Asia), 2024.
- F.2 Program Chair, the 20th China Fault Tolerant Computing Conference (CCF CFTC2023), July 28-30, 2023.
- F.3 Associate Editor, IEEE Transactions on Circuits and Systems II: Express Briefs, 2023-
- F.4 Editorial Committee, Journal of Electronics and Information Technology, China, 2023.01-2026.12
- F.5 Publicity Chair, Asian Hardware Oriented Security and Trust Symposium (AsianHOST) 2023
- F.6 Lead Guest Editor, “Advanced Integrated Circuits Technology”, Journal of Electronics and Information Technology, 2023
- F.7 Committee Vice Chair, CCF Chip Conference, 28-30 Jul., 2022.
- F.8 Program Chair, the 7th International Conference on Integrated Circuits and Microsystems (ICICM 2022)
- F.9 Lead Guest Editor: “In-memory Computing”, Journal of Electronics and Information Technology, 2022
- F.10 Program Chair, the 19th China Fault Tolerant Computing Conference (CCF CFTC2021)
- F.11 Lead Guest Editor: “Hardware Security”, Chinese Journal of Computers, 2021
- F.12 Lead Guest Editor: “Hardware Security”, Journal of Electronics and Information Technology, 2021
- F.13 Guest Editor, IEEE Transactions on Circuits and Systems II -Express Briefs, 2021
- F.14 Special Session Chair: Nano-Inspired Hardware Security, NANOARCH 2021
- F.15 Steering Member: Hardware Security Forum of China. 2021-
- F.16 Guest Editor: Hardware Security for Integrated Circuits, Journal of Network and Information Security, 2020
- F.17 Special Session Chair: Hardware Security, the 29th IEEE Asian Test Symposium (ATS2020)
- F.18 Panel Chair: The Five Hardware Security Forum of China, Xian, Aug. 21-22, 2020
- F.19 Editorial Board: International Journal of Cognitive Computing in Engineering, 2020.07-2022.07.
- F.20 Special Session Chair: Security and Privacy Issues in AI and Their Impacts on Hardware Security, the 30th edition of the ACM Great Lakes Symposium on VLSI (GLSVLSI2020)
- F.21 Poster Session Chair: Asian Hardware Oriented Security and Trust Symposium 2020.
- F.22 Special Session Organizer: the 30th edition of the ACM Great Lakes Symposium on VLSI (GLSVLSI2020).
- F.23 Session Co-Chair: the 21st International Symposium on Quality Electronic Design (ISQED2020)
- F.24 Guest Editor: Chinese Journal of Network and Information Security (CCF Ranked C), Special Issue on Hardware Security, Submission Deadline: Nov. 15, 2020

- F.25 Session Chair: CCF Design Automation Conference (DAC) 2020
- F.26 Poster Session Chair: AsianHOST2019.
- F.27 Guest Editor: Journal of Information Security and Applications (CCF Ranked C), Special Issue on Processing of encrypted data for privacy protection in cloud computing and other applications, Submission Deadline: April 30, 2019
- F.28 Guest Editor: Journal of Low Power Electronics and Applications, Special Issue on Energy-Aware Neuromorphic Hardware. Submission Deadline: May 1, 2018
- F.29 General Chair: The 4th China Hardware Security Forum, Beijing, China, 2019
- F.30 General Chair: The 3th China Hardware Security Forum, Harbin, China, 2018
- F.31 Program Chair: The 2th China Hardware Security Forum, Nanjing, China, 2017
- F.32 Session Chair: China Test Conference, 2018
- F.33 Seminar Chair: The 4th International Conference on Cloud Computing and Security (ICCCS 2018)
- F.34 Session Chair: The 15th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom2016)

Technical Program Committee Member

- F.35 ACM/IEEE Design Automation Conference (DAC) 2023
- F.36 Asian Hardware Oriented Security and Trust Symposium (AsianHOST) 2023
- F.37 IEEE 32nd Asian Test Symposium (ATS23)
- F.38 IEEE International Symposium on VLSI (ISVLSI 2023)
- F.39 IEEE 10th International Conference on Cyber Security and Cloud Computing (CSCloud2023)
- F.40 IEEE 9th International Conference on Edge Computing and Scalable Cloud (EdgeCom2023)
- F.41 Asia and South Pacific Design Automation Conference (ASP-DAC) 2020/2021/2022
- F.42 The 18th International Conference on Information Security and Cryptology 2022
- F.43 International Conference on Field-Programmable Technology (FPT) 2020
- F.44 International Symposium on Quality Electronic Design (ISQED) 2017/2018/2019/2020/2021/2022
- F.45 The 7th International Conference on Integrated Circuits and Microsystems 2022
- F.46 Asian Hardware Oriented Security and Trust Symposium (AsianHOST) 2019/2020/2021/2022
- F.47 China Fault Test Conference (CFTC) 2018/2019
- F.48 The ACM Great Lakes Symposium on VLSI (GLSVLSI) 2017
- F.49 China Electronic Design Automation (ChinaEDA) 2016/2017
- F.50 Workshop on Cloud Storage Service and Computing (WCSSC) 2016/2017
- F.51 Hardware security track of International Conference on Field-Programmable Technology (FPT) 2014

Invited Journal Review

- F.52 IEEE Transactions on Computers
- F.53 IEEE Transactions on Transactions on Information Forensics and Security
- F.54 IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems
- F.55 IEEE Transactions on Neural Networks and Learning Systems
- F.56 IEEE Transactions on Very Large-Scale Integration Systems
- F.57 ACM Transactions on Reconfigurable Technology and Systems
- F.58 ACM Transactions on Design Automation of Electronic Systems
- F.59 IEEE Transactions on Industrial Electronics
- F.60 IEEE Transactions on Circuits and Systems I: Regular Papers
- F.61 IEEE Transactions on Circuits and Systems II: Express Briefs
- F.62 ACM Journal on Emerging Topics in Computing Systems
- F.63 ACM Computing Surveys
- F.64 IEEE Signal Processing Letters
- F.65 IEEE Embedded Systems Letters
- F.66 Journal of Information Security and Application
- F.67 Integration, the VLSI Journal
- F.68 Canadian Journal of Electrical and Computer Engineering
- F.69 SCIENCE CHINA Information Sciences
- F.70 Chinese Journal of Electronics
- F.71 Electronics Letters

g. Ph.D. dissertation

“Security and Trust for FPGA-based Systems”, Hunan University, 2015. (**Outstanding Doctoral dissertation of Hunan University**)

3. Teaching, Mentoring, and Advising Activities

a. Courses Taught

- A.1 Authentication and Access Control Technologies (for undergraduate students), 2015, 2016
- A.2 Computer System Security (for undergraduate students), 2016, 2017
- A.3 Information Security Engineering (for undergraduate students), 2018
- A.4 Security System Experiments (for undergraduate students), 2018, 2019
- A.5 Trusted Computing (for undergraduate students), 2019, 2020, 2021, 2022
- A.6 System Security (for PhD student), 2020, 2021, 2022

