# Jiliang ZHANG

***IEEE/CCF Senior Member***

College of Computer Science and Electronic Engineering (CSEE)
Hunan University, Changsha 410082, China.

zhangjiliang@hnu.edu.cn
http://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 the CSEE, Hunan University, Changsha, China (90%)
Professor in the Peng Cheng Laboratory, Shenzhen, China (10%)

### 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

| | |
|---|---|
| 2021 | 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 New Faculty Award of Hunan University. |
| 2018 | Recipient of the Hu-Xiang Youth Talent, Hunan Province. |
| 2019 | Best Paper Nomination, the *18th China Fault Tolerant Computing Conference (CFTC)*. |
| 2017 | The High-level Talent in Shenyang City, Liaoning Province. |
| 2017 | The Third Prize of Shenyang Natural Science Academic Achievement Award. |
| 2017 | Best Paper Nomination, *18th International Symposium on Quality Electronic Design (ISQED)*. |
| 2013 | China Scholarship Council Scholarship. |
| 2012 | National Scholarship. |

### Students' Honors and Awards

| | |
|---|---|
| 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)** |
| 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/Hardware-assisted Security*: Physical unclonable functions; Hardware obfuscation; Hardware IP protection (watermarking, metering); FPGA Security; Hardware Trojan attacks and detection techniques; Hardware techniques to facilitate software and/or system security; Applications of hardware security to secure system and so on.

*Micro-Architecture Security: Cache Side-Channel Attacks and Countermeasures*

*Artificial Intelligence Security*: DNN security; Adversarial attacks and defenses.

*Software Security*: Code-reuse attacks and defenses.

**Summary:**

I have authored 34 journal articles and 24 conference papers, including 47 the first/corresponding author papers. Google Scholar Citations: 1170, H-index of the first/corresponding author papers: 20.

**a. Articles in Refereed Journals**

A.1 **Jiliang Zhang***, Chaoqun Shen, Haihan Su, Md Tanvir Arafin, Gang Qu, "Voltage Over-scaling-based Lightweight Authentication for IoT Security", ***IEEE Transactions on Computers***, 2021, DOI: 10.1109/TC.2021.3049543.

A.2 **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***, 2021

A.3 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***, 2021, DOI: 10.1109/TCSII.2021.3065292.

A.4 **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.

A.5 Junye Shi, Yang Lu, **Jiliang Zhang***, "Approximation Attacks on Strong PUFs", ***IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems***, vol. 39, no. 10, pp. 2138-2151, Oct. 2020. [PDF] [Source Code]

A.6 **Jiliang Zhang***, Gang Qu, "Physical Unclonable Function-based Key-Sharing via Machine Learning for IoT Security", ***IEEE Transactions on Industrial Electronics***, vol. 67, no. 8, pp. 7025–7033, Aug. 2020.

A.7 **Jiliang Zhang***, Chen Li, "Adversarial Examples: Opportunities and Challenges", ***IEEE Transactions on Neural Networks and Learning Systems***, vol. 31, no. 7, pp.2578-2593, July 2020. [Source Code]

A.8 **Jiliang Zhang***, Gang Qu, "Recent Attacks and Defenses on FPGA-based Systems", ***ACM Transactions on Reconfigurable Technology and Systems***, vol. 12, no. 3, Article No. 14, 24 pages, August 2019.

A.9 **Jiliang Zhang***, Binhang Qi, Zheng Qin, Gang Qu, "HCIC: Hardware-assisted Control-flow Integrity Checking", ***IEEE Internet of Things Journal*** , vol. 6, no. 1, pp. 458-471, Feb. 2019. (Citations: 29)

A.10 Aibin Yan, Kang Yang, Zhengfeng 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.

* Corresponding author, who leads the work.

A.11 **Jiliang Zhang***, Xiao Tan, Yuanjing 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.12 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.13 **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.14 **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)***, vol. 11, no. 11, pp. 2626-2627, Nov. 2016.

A.15 **Jiliang Zhang***, "A Practical Logic Obfuscation Technique for Hardware Security", ***IEEE Transactions on Very Large Scale Integration (VLSI) Systems (TVLSI)***, vol. 24, no. 3, pp. 1193-1197, March 2016. (Citations: 92)

A.16 **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)***, vol. 10, no. 6, pp. 1137-1150, June 2015. **(Citations: 119)**

A.17 **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, pp. 1-20, February 2015. **(Citations: 31)**

A.18 **Jiliang Zhang**, Xiao Tan, Xiangqi Wang, Aibin Yan*, Zheng Qin, "T2FA: Transparent Two-Factor Authentication", ***IEEE Access***, vol. 6, pp. 32677-32686, June 2018.

A.19 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***, 2020, DOI:10.26599/TST.2019.9010048.

A.20 Yaping Lin, Xinbo Liu, He Li, **Jiliang Zhang**, "A Novel Method for Malware Detection on ML-based Visualization Technique", *Computers & Security*, 2019, In Press.

A.21 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***, vol. 87, no.2, pp. 215-227, May 2017.

A.22 **Jiliang Zhang*** Weizheng Wang, Xingwei Wang, Zhihua Xia, "Enhancing Security of FPGA-based Systems with Combinational Logic Binding", ***Journal of Computer Science and Technology (JCST)***, vol. 32, no. 2, pp. 329-339, March 2017.

A.23 **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)***, vol. 31, no. 1, pp. 124-136, Jan. 2016.

A.24 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. **(Citations: 65)**

A.25 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, pp. 355-362, Sep. 2016.

A.26 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***, vol. 12, no. 6, pp. 1317-1321, June 2015.

A.27 Yipeng Ding*, Jingtian Tang, Xuemei Xu, **Jiliang Zhang**, "Echo Interference Suppression Approach for Doppler Through-Wall Radar", ***IEEE Sensors Journal***, vol. 15, no. 6, pp. 3395-3402, June 2015.

A.28 **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)***, vol. 29, no. 4, pp. 664-678, July 2014. **(Citations: 81)**

A.29 **Jiliang Zhang**, Yaping Lin*, Yongqiang Lyu, Xiangqi Wang, "A Chaotic-based Publicly Verifiable FPGA IP Watermark Detection Scheme", ***SCIENTIA SINICA Informationis*****, vol.43 no.9, pp.1096-1110**, 2013. (In Chinese)

A.30 **Jiliang Zhang***, Yaping Lin, Qiang Wu, Wenjie Che, "Watermarking FPGA Bitfile for Intellectual Property Protection", ***Radioengineering***, vol. 21, no. 2, pp. 764-771, June 2012.

A.31 **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)***, vol. 9, no. 22, pp. 1735-1741, Sep. 2012.

A.32 **Jiliang Zhang***, Yongqiang Lyu, Qiang Zhou, Qiang Wu, Yaping Lin, and Kang Zhao, "TimFastPlace: Critical-Path based Timing Driven FastPlace", ***IEICE Electronics Express (Elex)***, vol. 9, no. 16, pp. 1310-1315, Sep. 2012.

A.33 **Jiliang Zhang***, Yongqiang Lyu, Qiang Zhou, Qiang Wu, "A Sensitivity-Based Timing-Driven Fast Placement Algorithm", ***Chinese Journal of Electronics***, vol. 40, no. 12, pp. 2410-2414, 2012.

A.34 **Jiliang Zhang***, Qiang Wu, Jiani Chen, "Research on Design Method of Dynamic Partial Reconfigurable System", ***Journal of Software Engineering***, vol. 6, no. 2, pp. 21-30, 2012.

**b. Articles in Conference, Symposium, and Workshop Proceedings**

B.1 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.

B.2 **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.

B.3 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.

B.4 **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. (Invited Paper)

B.5 Yehao Kong, **Jiliang Zhang***, "Adversarial Audio: A New Information Hiding Method", The ***21st Conference of the International Speech Communication Association (INTERSPEECH)***, Shanghai, Oct. 2020.

B.6 **Jiliang Zhang***, Shuang Peng, Yupeng Hu, Fei Peng, Wei Hu, Jinmei Lai, Jing Ye, "HRAE: Hardware-assisted Randomization against Adversarial Example Attacks", in ***the 29th IEEE Asian Test Symposium***, 2020. (Invited Paper)

B.7 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.

B.8 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.

B.9 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.

B.10 **Jiliang Zhang***, Wuqiao Chen, "DeepCheck: Control-flow Integrity Checking based on Deep Learning", ***In 57th Design Automation Conference (DAC)***, San Francisco, CA, 2020 (DAC Work in Progress).

B.11 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. (Invited Paper)

B.12 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. (Invited Paper)

B.13 Xinbo Liu, **Jiliang Zhang***, Yaping Lin, He Li, "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.

B.14 Haihan Su, **Jiliang Zhang***, "Machine Learning Attacks on Voltage Over-scaling-based Lightweight Authentication", ***Asian Hardware Oriented Security and Trust Symposium (AsianHOST)***, Hongkong, China, Dec.17-18 2018.

B.15 Zihan Pang, **Jiliang Zhang***, Qiang Zhou, Shuqian Gong, et al., "Crossover Ring Oscillator PUF", ***The 18th International Symposium on Quality Electronic Design (ISQED)***, Santa Clara, CA, USA, March 14-15 2017. (Best Paper Nomination)

B.16 **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.

B.17 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.

B.18 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***, Xi'an, China, Aug.26-28 2015.

B.19 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***, Xi'an, China, Aug.26-28 2015.

B.20 **Jiliang Zhang***, Gang Qu, "A Survey on Security and Trust of FPGA-based Systems", ***In 13th International Conference on Field Programmable Technology (FPT'14)***, Shanghai, China, Dec. 10-12 2014.

B.21 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)***, Shanghai, China, Dec. 10-12 2014.

B.22 **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. 2-4 2013.

B.23 **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, April 28-30 2013.

B.24 **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)***, Guangzhou, China, Nov. 16-18 2013.

## c. Invited Talks and Professional Presentations

C.1 **(Invited Talks)** "PUF Design and Applications", CCF Advanced Computer Architecture (ACA2020), Computer System Security and Future Architecture Forum, 15 Aug., 2020.

C.2 **(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.3 **(Invited Talks)** "PUF Design and Applications", Beihang University (virtual), 30 Sept., 2020, Host: Zhenyu Guan.

C.4 **(Invited Talks)** "Hardware、Software and AI Security", Wuhan University, 25 Nov., 2019, Host: Ming Tang.

C.5 **(Invited Talks)** "Hardware Secure: Physical Unclonable Functions", Beijing Institute of Technology, Nanjing, 12 Nov., 2019, Host: An Wang.

C.6 **(Invited Talks)** "Turn the Dust into Glory: Design of Physical Unclonable Functions", Southeast University, Nanjing, 10 Aug., 2019, Host: Weiwei Shan.

C.7 **(Keynote)** "Hardware and Hardware-assisted Security", CACR Conference on Cryptography Chips (CryptoIC), Nanjing, 2019.

C.8 **(Keynote)** "Hardware and Hardware-assisted Security", International Software and Hardware Design and Implementation Forum, Guilin, 2019.

C.9 **(Invited Talks)** "Hardware and Hardware-assisted Security", Shenzhen University, Shenzhen, 29 July, 2019, Host: Bin Li.

C.10 **(Keynote)** "Hardware-assisted Security", The Third Hardware Security Forum of China, Harbin, Aug. 2018.

C.11 **(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.12 **(Keynote)** “PUF and Applications”, The First Hardware Security Forum of China, Nantong, Aug. 24, 2016.

C.13 **(Specially Invited Guest)** “Security for FPGA Systems”, Internet Conference of China (ICoC), TOP Conference/Journal paper Panel, Aug. 28, 2015.

C.14 **(Invited Talks)** “Physical Unclonable Functions and Applications”, Huawei Technologies Co Ltd, Shenzhen, Jan. 2015, Host: Yuliang Zhou.

C.15 **(Invited Talks)** “Physical Unclonable Functions and Applications”, Hardware Security workshop in China, Shenzhen, Jan. 2015.

## d. Contracts and Grants

D.1 “Design Methods and Applications of Physical Unclonable Security Chip”, Key Program of National Natural Science Foundation for Young Scholars, 01/2021~12/2024

D.2 “Hardware-assisted System Security”, Hunan Natural Science Foundation for Distinguished Young Scholars, 01/2020~12/2023

D.3 “Hardware-assisted techniques against code reuse attacks”, National Natural Science Foundation of China, Principal Investigator, Grant No. 61874042, 01/2019~12/2022

D.4 “Research and Development of Independent and Controllable Physical Unclonable Chip”, Key Research and Development Program of Hunan Province, China. Principal Investigator, Grant No. 2019GK2082, 01/2020~12/2021

D.5 The Hu-Xiang Youth Talent Program, Grant No. 2018RS3041, Principal Investigator, Grant No. 2018RS3041, 01/2019~12/2021

D.6 “Intellectual Property Protection for Programmable Chips”. Natural Science Foundation of Hunan Province, China. Principal Investigator, Grant No. 2018JJ3072, 01/2018~12/2020

D.7 “***bypass and verification”, Funded by Chinese National Key Laboratory of Science and Technology on Information System Security, 01/2019~12/2020.

D.8 “PUF and Voiceprint-based Transparent Two-Factor Authentication”. CCF-IFAA Research Fund, Principal Investigator, 03/2018~03/2019

D.9 “Research on PUF and Obfuscation-based Active Defense Techniques for FPGA System Security”, National Natural Science Foundation of China, Principal Investigator, Grant No. 61602107, 01/2017~12/2019

D.10 “Hardware Security”, Fundamental Research Funds for the central Universities of China, Principal Investigator, 05/2017 ~ 4/2022

D.11 “Hardware-assisted Software Security”, Fundamental Research Funds for the central Universities of China, Principal Investigator, Grant No. N161704006, 01/2017 ~ 12/2018.

D.12 “Active Defense Techniques for FPGA System Security”, Funded by Key Laboratory of Chinese Academy of Sciences, Principal Investigator, 06/2015~06/2020

D.13 “Security and Trust for FPGA-based Systems”, Funded by Key Laboratory of Computer Network and Information Integration, Ministry of Education, Principal Investigator, 06/2016 ~ 05/2018.

D.14 “Hardware/software security for smart devices”, Fundamental Research Funds for the central Universities of China, Principal Investigator, Grant No. L1517002, 09/2015~12/2015.

## e. CN Patents

E.1 Jiliang Zhang，Junjie Hou. “Physical Unclonable Functions-based Lightweight Key Sharing Method”. Patent application number：2019104511615

E.2 Jiliang Zhang. “Dynamic Multi-key obfuscation for PUF Structure and Authentication”. Patent application number：2018110527086

E.3 Jiliang Zhang，Binhang Qi，Xiangqi Wang. “Hardware-assisted Defense System and Method against Code Reuse Attack”. Patent application number：201710823354.3

E.4 Jiliang Zhang，Yuanjing Zhang，Xiangqi Wang. “A Highly Reliable Physical Unclonable Function and Response Generation Method”. Patent application number：201710718128.5

E.5 Jiliang Zhang，Rui Jin. “Defense System and Method against Code Reuse Attacks”. Patent authorization number. ZL201610388347.7, Patent authorization time：2018.10.23

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

### Conference Chair/Editor

Program Co-Chair, CCF CFTC2021

Guest Editor, IEEE Transactions on Circuits and Systems II -Express Briefs, 2021

Steering Member: Hardware Security Forum of China.

Special Session Chair: Hardware Security, the 29th IEEE Asian Test Symposium (ATS2020)

Panel Chair: The Five Hardware Security Forum of China, Xian, Aug. 21-22, 2020

Editorial Board: International Journal of Cognitive Computing in Engineering, 2020.07-2022.07.

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)

Session Co-Chair: the 21st International Symposium on Quality Electronic Design (ISQED2020)

Guest Editor: Chinese Journal of Network and Information Security (CCF Ranked C), Special Issue on Hardware Security, Submission Deadline: Nov. 15, 2020

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

Guest Editor: Journal of Low Power Electronics and Applications, Special Issue on Energy-Aware Neuromorphic Hardware. Submission Deadline: May 1, 2018

Session Chair: CCF Design Automation Conference (DAC) 2020

Poster Session Chair: Asian Hardware Oriented Security and Trust Symposium (AsianHOST) 2019

Chair: The Fourth Hardware Security Forum of China, Beijing, China, 2019

Chair: The Third Hardware Security Forum of China, Harbin, China, 2018

Session Chair: China Test Conference 2018

Workshop Chair: The 4th International Conference on Cloud Computing and Security (ICCCS 2018)

Program Chair: The Second Hardware Security Forum of China, Nanjing, China, 2017

Security Track Session (#04 and #06) Chair: The 15th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom2016)

### Program Committee Member

International Conference on Field-Programmable Technology (FPT) 2020

25th Asia and South Pacific Design Automation Conference (ASP-DAC) 2020/2021

International Symposium on Quality Electronic Design (ISQED) 2017/2018/2019/2020

China Conference on Data Mining (CCDM) 2020

Asian Hardware Oriented Security and Trust Symposium (AsianHOST) 2019

China Fault Test Conference (CFTC) 2018/2019/2020

The ACM Great Lakes Symposium on VLSI (GLSVLSI) 2017

China Electronic Design Automation (ChinaEDA) 2016/2017

Workshop on Cloud Storage Service and Computing (WCSSC) 2016/2017

Hardware security track of International Conference on Field-Programmable Technology (FPT) 2014

### Invited Journal Review

IEEE Transactions on Transactions on Information Forensics and Security

IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

IEEE Transactions on Neural Networks and Learning Systems

IEEE Transactions on Very Large-Scale Integration Systems

IEEE Transactions on Industrial Electronics

IEEE Consumer Electronics Magazine

IEEE Transactions on Circuits and Systems I

IEEE Transactions on Circuits and Systems II: Express Briefs

IEEE Transactions on Instrumentation & Measurement

ACM Computing Surveys

ACM Transactions on Reconfigurable Technology and Systems

ACM Transactions on Design Automation of Electronic Systems

ACM Journal on Emerging Topics in Computing Systems

CCF Transactions on High Performance Computing

IEEE Signal Processing Letters

IEEE Embedded Systems Letters

IEEE Access

Journal of Information Security and Application

Integration, the VLSI Journal

Peer-to-Peer Networking and Applications

International Journal of Machine Learning and Cybernetics

Canadian Journal of Electrical and Computer Engineering

SCIENCE CHINA Information Sciences

Chinese Journal of Electronics

Electronics Letters

Journal of Computer-Aided Design & Computer Graphics

International Journal of Bifurcation and Chaos

……

### 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), Fall 2015, Fall 2016

A.2 Computer System Security (for undergraduate students), Fall 2016

A.3 Information Security Engineering (for undergraduate students), Fall 2018

A.4 Security System Experiments (for undergraduate students), Spring 2018, 2019

A.5 Trusted Computing (for undergraduate students), Fall 2019, 2020

A.6 System Security (for PhD student), Fall 2020