Yue ZHENG

☎ +65 94264795 | ✉ yue.zheng@ntu.edu.sg | https://www.linkedin.cn/injobs/in/yue-zheng-603358b9

Research Interests

My research focuses on hardware security. I am interested to investigate the security and privacy vulnerabilities in intelligent, autonomous, and distributed computing systems, and develop hardware security based lightweight, energy-efficient, and comprehensive solutions.

Education

Doctor of Philosophy (PhD) in Electrical and Electronic Engineering *2015 - 2020*
NANYANG TECHNOLOGICAL UNIVERSITY *Singapore*

- Thesis: Physical Unclonable Function Based Solutions to Unification of User, Device and Data Authentication
- Advisor: Chang Chip Hong (IEEE Fellow)
- CGPA: 4.63/5

Bachelor of Engineering (BEng) in Communication Engineering *2011 - 2015*
SHANGHAI UNIVERSITY *China*

- CGPA: 3.88/4 (Ranking: 1/368)

Experience

2020-Now	**Research Fellow**, Nanyang Technological University, Singapore
2019-2020	**Project Officer**, Nanyang Technological University, Singapore
2019	**Visiting Scholar**, Kyoto University, Japan (Host: Takashi Sato)

Publications and Patents

JOURNALS

1. Y. Zheng, S. Wang, and C. H. Chang, “A DNN fingerprint for non-repudiable model ownership identification and piracy detection,” *IEEE Trans. Inf. Forensics Secur. (**TIFS, CCF-A**)*, July 2022
2. Y. Zheng, W. Liu, C. Gu, and C. H. Chang, “PUF-based mutual authentication and key exchange protocol for peer-to-peer IoT applications,” *IEEE Trans. Dependable Secure Comput. (**TDSC, CCF-A**)*, July 2022
3. Y. Cao, X. Zhao, W. Zheng, Y. Zheng, and C. H. Chang, “A new energy-efficient and high throughput two-phase multi-bit per cycle ring oscillator-based true random number generator,” *IEEE Trans. Circuit. Syst. Regular paper (**TCAS-I**)*, pp. 272–283, Jan. 2022
4. Y. Zheng, X. Zhao, T. Sato, Y. Cao, and C. H. Chang, “Ed-PUF: Event-driven physical unclonable function for camera authentication in reactive monitoring system,” *IEEE Trans. Inf. Forensics Secur. (**TIFS, CCF-A**)*, pp. 2824–2839, Mar. 2020
5. Y. Zheng, Y. Cao, and C. H. Chang, “A PUF-based data-device hash for tampered image detection and source camera identification,” *IEEE Trans. Inf. Forensics Secur. (**TIFS, CCF-A**)*, vol. 15, pp. 620–634, Jul. 2019
6. A. Cui, C. H. Chang, W. Zhou, and Y. Zheng, “A new PUF based lock and key solution for secure in-field testing of cryptographic chips,” *IEEE Trans. Emerging Topics in Comput. (**TETC**)*, pp. 1095–1105, Mar. 2019
7. Y. Zheng, Y. Cao, and C. H. Chang, “UDhashing: Physical unclonable function based user-device hash for endpoint authentication,” *IEEE Trans. Industrial Electronics (**TIE, Q1**)*, vol. 66, pp. 9559–9570, Jan. 2019
8. C. H. Chang, Y. Zheng, and L. Zhang, “A retrospective and a look forward: Fifteen years of physical unclonable function advancement,” *IEEE Circuits and Systems Magazine (**CASM**)*, vol. 17, pp. 32–62, Aug. 2017

Conferences

1. C. Xu, W. Liu, Y. Zheng, S. Wang, and C. H. Chang, “Inconspicuous data augmentation based backdoor attack on deep neural networks,” in *Proc. IEEE. Int. System-On-Chip Conf. (**SOCC**)*, (Belfast, Northern Ireland), Sept. 2022
2. S. Wang, C. Xu, Y. Zheng, and C. H. Chang, “A buyer-traceable DNN model IP protection method against piracy and misappropriation,” in *Proc. IEEE Int. Conf. Artificial Intell. Circuits Syst. (**AICAS**)*, (Incheon, Korea), Jun. 2022
3. Y. Zheng and C. H. Chang, “Secure mutual authentication and key-exchange protocol between PUF-embedded IoT endpoints,” in *Proc. IEEE Int. Symp. Circuits Syst. (**ISCAS**)*, (Daegu, Korea), May 2021
4. J. X. Soo, Y. Zheng, and C. H. Chang, “Live Demonstration: Event-driven physical unclonable function for camera authentication in reactive monitoring system,” in *Proc. IEEE Int. Symp. Circuits Syst. (**ISCAS**)*, (Daegu, Korea), May 2021 (J.X. Soo is a second year undergraduate under my guidance)
5. B. Wang, X. Zhao, Y. Zheng, and C. H. Chang, “An in-pixel gain amplifier based event-driven physical unclonable function for CMOS dynamic vision sensors,” in *Proc. IEEE Int. Symp. Circuits Syst. (**ISCAS**)*, (Hokkaiddo, Japan), May 2019
6. Y. Zheng, S. S. Dhabu, and C. H. Chang, “Securing IoT monitoring device using PUF and physical layer authentication,” in *Proc. IEEE Int. Symp. Circuits Syst. (**ISCAS**)*, (Florence, Italy), May 2018
7. S. S. Dhabu, Y. Zheng, W. Liu, and C. H. Chang, “Active IC metering of digital signal processing subsystem with two-tier activation for secure split test,” in *Proc. IEEE Int. Symp. Circuits Syst. (**ISCAS**)*, (Florence, Italy), May 2018
8. Y. Zheng, Y. Cao, and C. H. Chang, “Facial biohashing based User-Device physical unclonable function for bring your own device system (Invited Paper),” in *Proc. IEEE Int. Conf. Consumer Electronics. (**ICCE**)*, (Las Vegas, USA), Jan. 2018
9. Y. Cao, C. H. Chang, and Y. Zheng, “An energy-efficient true random number generator based on current starved ring oscillators,” in *Proc. IEEE Asian Hardware-Oriented Secur. Trust (**AsianHOST**) Symposium*, (Beijing), Oct. 2017 (Cisco Best Paper Award Candidate)
10. C. Liu, Y. Zheng, and C. H. Chang, “A new write-contention based dual-port SRAM PUF with multiple response bits per cell,” in *Proc. IEEE Int. Symp. Circuits Syst. (**ISCAS**)*, (Baltimore, USA), May 2017
11. Y. Zheng, Y. Cao, and C. H. Chang, “A new event-driven dynamic vision sensor based physical unclonable function for camera authentication in reactive monitoring system,” in *Proc. 2016 IEEE Asian Hardware-Oriented Secur. Trust (**AsianHOST**) Symposium*, (Taiwan), pp. 1–6, Dec. 2016

Patent & Invited Media Release

1. Y. Zheng, C. H. Chang, and W. Liu, “PUF-based Mutual Authentication and Key-Exchange,” *Invention disclosure ref. 2021-336-01-SG PRV, **Singapore Provisional Patent** Application No. 10202107780Q filed on 15 July 2021 and **US Patent** Application No: 17/866,332, filed on July 15, 2022*
2. “Can BYOD be as Secure as Company-Owned Devices?,” ***IEEE Xplore Innovation Spotlight***, Aug. 2018. [Online; Accessed 2022-Jul-4] `https://innovate.ieee.org/innovation-spotlight/biohashing-physical-unclonable-function-byod-authentication-scheme/`

Selected Awards

2021	**Women in Engineering, Science, and Technology (WiEST) Conference Grant Award**, NTU	*9 awarded*
2017	**People’s Choice Award**, Three Minute Thesis (3MT) Competition, Singapore Final	*Top 4*
2017	**People’s Choice Award**, Three Minute Thesis (3MT) Competition, NTU	*Top 4*
2015-2019	**Research Scholarship**, NTU	
2015	**Outstanding Graduates of Shanghai**, Shanghai Municipal Education Commission	
2015	**Excellent Bachelor Dissertation Award**, Shanghai University	
2014	**China National Scholarship**, The Central Government of China	*Top 0.2%*
2012-2015	**Outstanding Academic Scholarship**, Shanghai University	*Top 1%*

Academic Services & Professional Development

Services

2022-2023	**Associate Editor**, Transactions on Circuits and Systems II: Express Briefs
2022	**Special Session Chair**, ISOCC
2022	**Track Chair**, APCCAS
2022	**PhD Forum Chair**, AsianHOST
2022	**Session Chair**, AICAS
2021-2022	**Reviewer Committee Member**, ISCAS
2021	**Track Chair, Session Chair**, VLSI-SoC
2021	**Session Chair**, ISCAS
2021	**VSA-TC member**, VLSI Systems and Applications Technical Committee member
2021	**Technical Program Committee member**, SECURWARE 2021

Development

1. **The Alpha and Omega of Side Channel Attack: from DPA to Deep Learning**
   by Lejla Batina & Stjepan Picek, 26-29 April 2021 (Online Workshop supported by WiEST award)

2. **Cryptography I**
   by Dan Boneh, 2021 (Coursera)

3. **Python - The Practical Guide**
   by Maximilian Schwarzmuller, June 2020 (Udemy)

4. **AI Summer School**
   22-26 July, 2019 (Offline workshop at National University of Singapore)

5. **Machine Learning**
   by Andrew Ng, 2016 (Coursera)

Reviewer

2022	**TETC**, Transactions on Emerging Topics in Computing
2022	**TII**, Transactions on Industrial Informatics
2022	**TCAS-II**, Transactions on Circuits and Systems II: Express Briefs
2021	**TCAS-I**, Transactions on Circuits and Systems I
2021	**TIFS**, Transactions on Information Forensics and Security
2021-2022	**TDSC**, Transactions on Dependable and Secure Computing
2021	**TVLSI**, Transactions on VLSI Systems
2021	**JETCAS**, Journal on Emerging and Selected Topics in Circuits and Systems
2020-2021	**HOST**, Hardware Oriented Security and Trust Symposium
2020-2021	**ASHES**, Attacks and Solutions in Hardware Security Workshop
2017-2021	**ISCAS**, International Symposium on Circuits and Systems
2017-2021	**AsianHOST**, Asian Hardware Oriented Security and Trust Symposium

Talks and Special Sessions

Invited Talks, Tutorials and Special Sessions

1. **Tutorial Speaker: ISCAS, 2021**
   Defender-Adversary Arms Race of Logic Locking – Part I
2. **Invited Speaker: Zhejiang University, 2020**
   PUFs Based Solutions to Unification of User, Device, Data Authentication
3. **Invited Speaker: CCF China Test Conference, Xi'an, Shan Xi, 2020**
   A Dynamic Vision Sensor Based Event-Driven PUF
4. **Special Session Organizer: ISCAS, 2021**
   Hardware Security in the New Wave of Digital Technology Revolution
5. **Special Session Organizer: AICAS, 2022**
   Security and Privacy in Deployment of Deep Neural Networks

Conference Presentations

1. **ISCAS 2021**, *Secure mutual authentication and key-exchange protocol between PUF-embedded IoT endpoints*
2. **ISCAS 2018**, *Securing IoT monitoring device using PUF and physical layer authentication*
3. **ICCE 2018**, *Facial biohashing based User-Device physical unclonable function for bring your own device*
4. **AsianHOST 2016**, *A new event-driven dynamic vision sensor based physical unclonable function for camera authentication in reactive monitoring system*

Teaching Experience

2017-2018	**EEE Escape Room Project "Xperience@EEE"**, Teaching Assistant
2017-2018	**Engineering Mathematics**, Teaching Assistant

Mentees

2021-2022	**Xu Kangwei**, Beihang Univ., CASS Mentoring Programme @ APCCAS 2021
2021-2022	**Tan Yi Xian**, SCBE, NTU, CN Yang Scholarship Programme
2021-2022	**Noah Winston NG**, EEE, NTU, Final Year Project
2021-2022	**Andy Ong Wei Wang**, EEE, NTU, Final Year Project
2021-2022	**Peh Jia Ming**, EEE, NTU, Final Year Project
2019-2020	**Soo Jian Xian**, EEE, NTU, CN Yang Scholarship Programme
2018-2019	**Law Jian Hwee Sherman**, EEE, NTU, Final Year Project
2017-2018	**Teo Wang Wei**, EEE, NTU, URECA (Undergraduate Research Experience on CAmpus), FYP
2017-2018	**Chen Hao**, EEE, NTU, Final Year Project
2016-2017	**Kristianto Wirawan**, EEE, NTU, Final Year Project