Chenglu Jin **Updated: August, 2020**

CONTACT INFORMATION
370 Jay Street, 13th Floor
Brooklyn, NY 11201
Email: chenglu.jin@nyu.edu
Website: chenglujin.github.io

CURRENT POSITION
Research Assistant Professor at **NYU Center for Cybersecurity**
Joint appointment at **NYU Center for Urban Science and Progress**

EDUCATION

University of Connecticut Storrs, CT, USA

Ph.D., Electrical Engineering, GPA: 4.08/4.0 Aug'19

- Dissertation: *Cryptographic Solutions for Cyber-Physical System Security*
- Advisor: Prof. Marten van Dijk

New York University Brooklyn, NY, USA

M.S., Computer Engineering, GPA: 3.91/4.0 May'14

- Thesis: *NREPO: Normal Basis Recomputing with Permuted Operands*
- Advisor: Prof. Ramesh Karri

Xidian University Xi'an, China

B.S., Electronic Information Science and Technology, GPA: 85/100 Jun'12

WORK AND RESEARCH EXPERIENCES

New York University Mar'20 to Present
Research Assistant Professor at CUSP and CCS Brooklyn, NY, USA

New York University Sep'19 to Feb'20
Smart Cities Postdoctoral Associate at CUSP and CCS Brooklyn, NY, USA
Advisers: Prof. Ramesh Karri and Prof. Daniel Neill

University of Connecticut Aug'14 to Aug'19
Research Assistant Storrs, CT, USA
Adviser: Prof. Marten van Dijk

Singapore University of Technology and Design May'18 to Aug'18
Intern at iTrust Singapore
Mentor: Prof. Jianying Zhou

Open Security Research Jun'16 to Aug'16
Intern Shenzhen, China
Mentor: Dr. Junfeng Fan

Open Security Research, Shenzhen, China Jun'15 to Aug'15
Intern Shenzhen, China
Mentor: Dr. Junfeng Fan

New York University Sep'13 to May'14
Research Assistant Brooklyn, NY, USA
Adviser: Prof. Ramesh Karri

Publications * denotes that the authors are in alphabetical order.

Book Chapters

1. R. S. Khan, N. Noor, **C. Jin**, J. Scoggin, Z. Woods, S. Muneer, A. Ciardullo, P. H. Nguyen, A. Gokirmak, M. van Dijk, and H. Silva. (2017) "Phase Change Memory and its Application in Hardware Security". In *Security Opportunities in Nano Devices and Emerging Technologies*. CRC Press.

Journals

2. P. H. Nguyen, D. P. Sahoo, **C. Jin**, K. Mahmood, U. Rührmair, and M. van Dijk. (2019) "The Interpose PUF: Secure PUF Design against State-of-the-art Machine Learning Attacks". In *IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)*. (Acceptance rate of Issue 4: **9/66 = 13.6%**. Overall acceptance rate of Volume 2019: **42/214 = 19.7%**)

3. **C. Jin**, and M. van Dijk. (2019) "Secure and Efficient Initialization and Authentication Protocols for SHIELD". In *IEEE Transactions on Dependable and Secure Computing (TDSC)*. (Impact factor: **6.404**)

4. S. K. Haider, **C. Jin**, M. Ahmad, D. M. Shila, O. Khan, and M. van Dijk. (2019) "Advancing the State-of-the-Art in Hardware Trojans Detection". In *IEEE Transactions on Dependable and Secure Computing (TDSC)*. (Impact factor: **6.404**)
   - **Featured in the Jan/Feb 2019 Issue of IEEE TDSC**

5. **C. Jin**, C. Herder, L. Ren, P. H. Nguyen, B. Fuller, S. Devadas, and M. van Dijk. (2017). "FPGA Implementation of a Cryptographically-Secure PUF based on Learning Parity with Noise". In *Cryptography*.
   - **Demonstrated as "Practical Cryptographically-Secure PUFs based on Learning Parity with Noise" at IEEE HOST 2017**

6. X. Guo, **C. Jin**, C. Zhang, A. Papadimitriou, D. Hély, and R. Karri. (2016) "Can Algorithm Diversity in Stream Cipher Implementation Thwart (Natural and) Malicious Faults?". In *IEEE Transactions on Emerging Topics in Computing (TETC)*. (Impact factor: **4.989**)

7. X. Guo, D. Mukhopadhyay, **C. Jin**, and R. Karri. (2015) "Security Analysis of Concurrent Error Detection against Differential Fault Analysis". In *Journal of Cryptographic Engineering (JCEN)*.

Conferences and Workshops

8. Z. Yang, **C. Jin**, Y. Tian, J. Lai, J. Zhou. (2020, Oct) "LiS: Lightweight Signature Schemes for Continuous Message Authentication in Cyber-Physical Systems". In *2020 ACM Asia Conference on Computer and Communications Security (AsiaCCS)*. (Acceptance rate of the 1st deadline: **9/64 = 14.1%**. Overall acceptance rate in 2020: **67/308 = 21.8%**)

9. **C. Jin***, Z. Yang*, M. van Dijk, and J. Zhou. (2019, Dec) "Proof of Aliveness". In *2019 Annual Computer Security Applications Conference (ACSAC)*. (Acceptance rate: **60/266 = 22.6%**)
   - **Artifacts Evaluated by the Committee**

10. R. S. Khan, N. Noor, **C. Jin**, S. Muneer, F. Dirisaglik, A. Cywar, P. H. Nguyen, M. van Dijk, A. Gokirmak, and H. Silva. (2019, Jul) "Exploiting Lithography Limits for Hardware Security Applications". In *2019 IEEE Conference on Nanotechnology (IEEE-NANO)*.
    - **Best Paper Award Candidate**

11. **C. Jin**, S. Valizadeh, and M. van Dijk. (2018, May) "Snapshotter: Lightweight Intrusion Detection and Prevention System for Industrial Control Systems". In *2018 IEEE International Conference on Industrial Cyber-Physical Systems (ICPS)*.

12. M. van Dijk*, **C. Jin***, H. Maleki*, P. H. Nguyen*, and R. Rahaeimehr*. (2018, Feb) "Weak-Unforgeable Tags for Secure Supply Chain Management". In *2018 International Conference on Financial Cryptography and Data Security (FC)*. (Acceptance rate for full papers: **27/110 = 24.5%**)

13. W. Yan, **C. Jin**, F. Tehranipoor, and J. Chandy. (2017, Sep) "Phase Calibrated Ring Oscillator PUF Design and Implementation on FPGAs". In *2017 International Conference on Field-Programmable Logic and Applications (FPL)*. (Acceptance rate for full papers: **49/208 = 23.6%**)

14. S. K. Haider, **C. Jin**, and M. van Dijk. (2017, Aug) "Advancing the State-of-the-Art in Hardware Trojans Design". In *2017 IEEE International Midwest Symposium on Circuits and Systems (MWSCAS)*.

15. H. Maleki, R. Rahaeimehr, **C. Jin**, and M. van Dijk. (2017, May) "New Clone-Detection Approach for RFID-Based Supply Chains". In *2017 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*. (Acceptance rate for full papers: **18/106 = 17.0%**)

16. **C. Jin**, L. Ren, X. Liu, P. Zhang, and M. van Dijk. (2017, Apr) "Mitigating Synchronized Hardware Trojan Attacks in Smart Grids". In *2017 Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG@CPSWeek)*.

17. X. Guo, N. Karimi, F. Regazzoni, **C. Jin**, and R. Karri. (2015, May) "Simulation and Analysis of Negative-Bias Temperature Instability Aging on Power Analysis Attacks". In *2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. (Acceptance rate for full papers: **17/71 = 23.9%**)

18. X. Guo, D. Mukhopadhyay, **C. Jin**, and R. Karri. (2014, May) "NREPO: Normal Basis Recomputing with Permuted Operands". In *2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*. (Acceptance rate for full papers: **18/65 = 27.7%**)

Patents

19. **C. Jin**, Z. Yang, M. van Dijk, and J. Zhou. (2019, Oct) "Proof of Aliveness in CPS by TOTP". *Singapore Patent Application No. 10201910114Y*. Filed

Pre-prints

20. P. Mahesh, A. Tiwari, **C. Jin**, P. R. Kumar, A. L. N. Reddy, S. T. S. Bukkapatanam, N. Gupta, and R. Karri. (2020) "A Survey of Cybersecurity and Resilience of Digital Manufacturing". *arXiv*.

21. **C. Jin**, V. Gohil, R. Karri, and J. Rajendran. (2020) "Security of Cloud FPGAs: A Survey". *arXiv*.

22. M. Linares, N. Aswani, G. Mac, **C. Jin**, F. Chen, N. Gupta, and R. Karri. (2020) "HACK3D: Evaluating Cybersecurity of Additive Manufacturing by Crowdsourcing". *arXiv*.

23. **C. Jin***, Z. Yang*, S. Adepu, and J. Zhou. (2019) "HMAKE: Legacy-Compliant Multi-factor Authenticated Key Exchange from Historical Data". *Cryptography ePrint Archive*.

24. **C. Jin**, M. van Dijk, M. Reiter, and H. Zhang. (2018) "PwoP: Intrusion-Tolerant and Privacy-Preserving Sensor Fusion". *Cryptography ePrint Archive*.

25. Y. Gao*, **C. Jin***, J. Kim, H. Nili, X. Xu, W. Burleson, O. Kavehei, M. van Dijk, D. C. Ranasinghe, and U. Rührmair. (2018) "Efficient Erasable PUFs from Programmable Logic and Memristors". *Cryptography ePrint Archive*.

26. R. S. Khan, N. Kanan, **C. Jin**, J. Scoggin, N. Noor, S. Muneer, F. Dirisaglik, P. H. Nguyen, H. Silva, M. van Dijk, and A. Gokirmak. (2017) "Intrinsically Reliable and Lightweight Physical Obfuscated Keys". *arXiv*.

27. **C. Jin**, X. Xu, W. Burleson, U. Rührmair, and M. van Dijk. (2015) "PLayPUF: Programmable Logically Erasable PUFs for Forward and Backward Secure Key Management". *Cryptography ePrint Archive*.

Awards

- Best Paper Award Candidate — IEEE-NANO 2019
- First Place Overall — MITRE eCTF 2017
- Iron Flag Award — MITRE eCTF 2017
- Doctoral Dissertation Fellowship — UConn Graduate School 2019
- Predoctoral Summer Research Fellowship — UConn ECE Dept. 2017
- Student Travel Award — CHES 2019
- Student Scholarship — BlackHat USA 2017
- Student Travel Award — HOST 2017
- Student Travel Award — Real World Crypto 2016

Teaching Experiences

New York University — Brooklyn, NY, USA

Course Co-developer:
- *Cybersecurity in Additive Manufacturing* — Fall 2020

Master Capstone Project Mentor:
- *Urban Science Intensive* — Spring 2020, Summer 2020

Teaching Assistant:
- *Introduction to Hardware Security and Trust* — Spring 2020
- *Advanced Computer Hardware Design* — Fall 2019

University of Connecticut — Storrs, CT, USA

Instructor and Course Developer:
- *Seminar on Cyber-Physical System Security* — Spring 2019

Course Co-developer:
- *Advanced Microprocessor Application Lab* — Spring 2017
- *Introduction to Hardware Security and Trust* — Spring 2017

Teaching Assistant:
- *Microprocessor Applications Laboratory* — Spring 2016, Fall 2016

Students

New York University — Brooklyn, NY, USA

Master Students:
- Shreeraman Arunachalam Karikalan, 2020
- Aparna Bhutani, 2020
- Siqi Huang, 2020
- Vivek Patel, 2020
- Guilherme Louzada, 2020
- Chenjie Su, 2020
- Akash Yadav, 2020
- Eric Zhuang, 2020

Professional Services

Program Committee Member

- Workshop on Attacks and Solutions in Hardware Security (ASHES'20)
- Int. Conference on Information and Communications Security (ICICS'19, 20)
- International Symposium on Quality Electronic Design (ISQED'20)
- International Conference on Science of Cyber Security (SciSec'19)

Student Program Committee Member

- IEEE Symposium on Security and Privacy (S&P'16)

Reviewer

Journals

- IEEE Transactions on Information Forensics and Security (TIFS)
- IEEE Transactions on Dependable and Secure Computing (TDSC)
- IEEE Transactions on Power Systems (TPWRS)
- IEEE Tran. on Computer-Aided Design of Integrated Circuits and Systems (TCAD)
- IEEE Transactions on Very Large Scale Integration Systems (TVLSI)
- IEEE Internet of Things Journal (IOT-J)
- IEEE Consumer Electronics Magazine (CEM)
- ACM Computing Surveys (CSUR)
- ACM Transactions on Reconfigurable Technology and Systems (TRETS)
- ACM Transactions on Design Automation of Electronic Systems (TODAES)
- ACM Journal on Emerging Technologies in Computing Systems (JETC)
- IOS Journal of Computer Security (JCS)
- Springer Journal of Hardware and Systems Security (HASS)
- IET Circuits, Devices & Systems
- MDPI Electronics
- MDPI Sensors
- MDPI Applied Sciences
- Journal of Internet Technology (JIT)

Conferences

- ACM/EDAC/IEEE Design Automation Conference (DAC'18, 19, 20)
- IEEE International Midwest Symposium on Circuits and Systems (MWSCAS'18)
- Cryptographers' Track at the RSA Conference (CT-RSA'17)

Sub-Reviewer

Journals

- IEEE Transaction on Computers (TC)
- Nature Communications
- Journal of Manufacturing Systems (JMS)
- IEEE Tran. on Computer-Aided Design of Integrated Circuits and Systems (TCAD)

Conferences

- International Test Conference (ITC'20)
- ACM/EDAC/IEEE Design Automation Conference (DAC'15, 16, 17, 20)
- ACM conference on Computer and Communications Security (CCS'17, 19)
- IEEE Int. Symp. on Hardware-Oriented Security and Trust (HOST'15, 16, 17, 18)
- IEEE International Conference on Computer Design (ICCD'16, 17)
- IEEE Symposium on Security and Privacy (S&P'17)
- ACM Great Lakes Symposium on VLSI (GLSVLSI'17)
- Theory of Implementation Security Workshop (TIs'16)

Competition Experiences

MITRE Embedded System CTF 2017 (**First Place Overall**, **Iron Flag Award**)
The goal of this competition was to build a secure bootloader for a microcontroller. Each team was required to design their own secure bootloader and attack the bootloaders designed by the other teams. Competitors are CMU, NEU, RPI, WPI, UMass, etc.

- Designed encryption and integrity checking scheme of our secure bootloader with side channel resistance.
- Found flaws in the encryption and integrity checking scheme of other teams' bootloaders.
- Won **First Place Overall** counting all the points gained by attacks and defenses.
- Won **Iron Flag Award** for successfully designing a secure system that defended every flag from its attackers in the whole competition.

Talks

1. Enhancing Cyber-Physical Systems Security with Cryptography and Hardware Security Primitives. *ECE Department Seminar.* Iowa State University, Ames, IA, USA, 2020/2.
2. Securing the Infrastructures in Smart Cities with Cryptography and Hardware Primitives. *Seminar.* Virginia Commonwealth University, Richmond, VA, USA, 2020/2.
3. Securing the Infrastructures in Smart Cities using Cryptography and Hardware Primitives. *Research Seminar.* Villanova University, Villanova, PA, USA, 2020/2.
4. Securing the Infrastructures in Smart Cities. *Center for Urban Science and Progress (CUSP) Research Seminar.* New York University, Brooklyn, NY, USA, 2019/9.
5. The Interpose PUF: Secure PUF Design against State-of-the-art Machine Learning Attacks. *Conference on Cryptographic Hardware and Embedded Systems (CHES).* Atlanta, GA, USA, 2019/8.
6. Enhancing Cyber-Physical System Security with Cryptography and Hardware Security Primitives. *Seminar.* Tennessee State University, Nashville, TN, USA, 2019/3.
7. Efficient Erasable PUFs from Programmable Logic and Memristors. *Connecticut Microelectronics and Optoelectronics Consortium Symposium.* University of New Haven, Orange, CT, USA, 2019/3.
8. Enhancing Cyber-Physical System Security with Cryptography and Hardware Security Primitives. *Seminar.* California State University, Long Beach, CA, USA, 2019/3.
9. Enhancing Cyber-Physical System Security with Cryptographic Primitives. *Seminar.* DePaul University, Chicago, IL, USA, 2019/2.
10. Enhancing Cyber-Physical System Security with Cryptography and Hardware Security Primitives. *Graduate Seminar.* University of Utah, Salt Lake City, UT, USA, 2019/2.
11. Cryptographic Solutions for Cyber-Physical System Security. *Seminar.* United Technologies Research Center, East Hartford, CT, USA, 2018/9.
12. PwoP: Intrusion-Tolerant and Privacy-Preserving Sensor Fusion. *Security Seminar.* University of Connecticut, Storrs, CT, USA, 2018/9.
13. Secure Sensor Fusion. *Modular Approach to Cloud Security (MACS) Project Meeting.* Boston University, Boston, MA, USA, 2018/1.

14. Advancing the State-of-the-Art in Hardware Trojans Design. *IEEE International Midwest Symposium on Circuits and Systems (MWSCAS)*. Medford, MA, USA, 2017/8.

15. Mitigating Synchronized Hardware Trojan Attacks in Smart Grids. *Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG)*. Pittsburgh, PA, USA, 2017/4.

16. Secure and Efficient Initialization and Authentication Protocols for SHIELD. *Security Seminar*. University of Connecticut, Storrs, CT, USA, 2016/9.

17. NREPO: Normal Basis Recomputing with Permuted Operands. *IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*. Washington, DC, USA, 2014/5.