

CONTACT INFORMATION	Science Park 123, 1098 XG Amsterdam, Netherlands	Email: chenglu.jin@cw.nl Website: chenglujin.github.io
CURRENT POSITION	Tenure-track Researcher at Centrum Wiskunde & Informatica (CWI Amsterdam) , the national research institute for mathematics and computer science in the Netherlands	
EDUCATION	University of Connecticut	Storrs, CT, USA
	Ph.D., Electrical Engineering, GPA: 4.08/4.0	Aug'19
	<ul style="list-style-type: none"> Dissertation: <i>Cryptographic Solutions for Cyber-Physical System Security</i> Advisor: Prof. Marten van Dijk 	
	New York University	Brooklyn, NY, USA
	M.S., Computer Engineering, GPA: 3.91/4.0	May'14
	<ul style="list-style-type: none"> Thesis: <i>NREPO: Normal Basis Recomputing with Permuted Operands</i> 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	Centrum Wiskunde & Informatica (CWI Amsterdam)	Oct'20 to Present
	Tenure-track Researcher in the Computer Security Group	Amsterdam, Netherlands
	New York University	Mar'20 to Aug'20
	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 in the ECE Department	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	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	
FUNDING	New York University , Brooklyn, NY, USA	
	<ul style="list-style-type: none"> US ARMY STTR: Fully-digital mmWave Lens-Antenna System for Resilient Tactical Communications (Phase I awarded: \$166K. Role: Co-PI.) 	

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. M. Linares, N. Aswani, G. Mac, **C. Jin**, F. Chen, N. Gupta, and R. Karri. (2021) “HACK3D: Crowdsourcing the Assessment of Cybersecurity in Digital Manufacturing”. In *IEEE Computer*.
3. P. Mahesh, A. Tiwari, **C. Jin**, P. R. Kumar, A. L. N. Reddy, S. T. S. Bukkapatnam, N. Gupta, and R. Karri. (2021) “A Survey of Cybersecurity of Digital Manufacturing”. In *Proceedings of the IEEE (PIEEE)*.
4. P. H. Nguyen, D. P. Sahoo, **C. Jin**, K. Mahmood, U. Rüßmair, 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: $42/214 = 19.7\%$)
5. **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)*.
6. 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)*.
 - Featured in the Jan/Feb 2019 Issue of IEEE TDSC
7. **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
8. 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)*.
9. 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

10. 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: $67/308 = 21.8\%$)
11. **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

12. 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

13. **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)*.
14. 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: $27/110 = 24.5\%$)
15. 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: $49/208 = 23.6\%$)
16. 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)*.
17. 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: $18/106 = 17.0\%$)
18. 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: $17/71 = 23.9\%$)
19. 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: $18/65 = 27.7\%$)

WORKSHOPS

20. Z. Yang, C. Yin, **C. Jin**, J. Ning, and J. Zhou. (2021, Jun) “Lightweight Delegated Authentication with Identity Fraud Detection for Cyber-physical Systems”. In *2021 ACM Cyber-Physical System Security Workshop (CPSS@AsiaCCS)*.
21. **C. Jin**, W. Burleson, M. van Dijk, and U. Rührmair. (2020, Nov) “Erasable PUFs: Formal Treatment and Generic Design”. In *2020 Workshop on Attacks and Solutions in Hardware Security (ASHES@CCS)*.
22. **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)*.

PATENTS

23. **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	<p>24. M. van Dijk*, D. Gurevin*, C. Jin*, O. Khan*, and P. H. Nguyen*. (2021) “Autonomous Secure Remote Attestation even when all Used and to be Used Digital Keys Leak”. <i>Cryptography ePrint Archive</i>.</p> <p>25. C. Jin, V. Gohil, R. Karri, and J. Rajendran. (2020) “Security of Cloud FPGAs: A Survey”. <i>arXiv</i>.</p> <p>26. C. Jin*, Z. Yang*, S. Adepu, and J. Zhou. (2019) “HMAKE: Legacy-Compliant Multi-factor Authenticated Key Exchange from Historical Data”. <i>Cryptography ePrint Archive</i>.</p> <p>27. C. Jin, M. van Dijk, M. Reiter, and H. Zhang. (2018) “PwoP: Intrusion-Tolerant and Privacy-Preserving Sensor Fusion”. <i>Cryptography ePrint Archive</i>.</p>	
AWARDS	<ul style="list-style-type: none"> • Best Paper Award Candidate • First Place Overall • Iron Flag Award • Doctoral Dissertation Fellowship • Predoctoral Summer Research Fellowship • Student Travel Award • Student Scholarship • Student Travel Award • Student Travel Award 	<p>IEEE-NANO 2019</p> <p>MITRE eCTF 2017</p> <p>MITRE eCTF 2017</p> <p>UConn Graduate School 2019</p> <p>UConn ECE Dept. 2017</p> <p>CHES 2019</p> <p>BlackHat USA 2017</p> <p>HOST 2017</p> <p>Real World Crypto 2016</p>
TEACHING EXPERIENCES	<p>New York University</p> <p>Course Co-developer:</p> <ul style="list-style-type: none"> • <i>Cybersecurity in Additive Manufacturing</i> <p>Master Capstone Project Mentor:</p> <ul style="list-style-type: none"> • <i>Urban Science Intensive</i> <p>Teaching Assistant:</p> <ul style="list-style-type: none"> • <i>Introduction to Hardware Security and Trust</i> • <i>Advanced Computer Hardware Design</i> <p>University of Connecticut</p> <p>Instructor and Course Developer:</p> <ul style="list-style-type: none"> • <i>Seminar on Cyber-Physical System Security</i> <p>Course Co-developer:</p> <ul style="list-style-type: none"> • <i>Advanced Microprocessor Application Lab</i> • <i>Introduction to Hardware Security and Trust</i> <p>Teaching Assistant:</p> <ul style="list-style-type: none"> • <i>Microprocessor Applications Laboratory</i> 	<p>Brooklyn, NY, USA</p> <p>Fall 2020</p> <p>Spring 2020, Summer 2020</p> <p>Spring 2020</p> <p>Fall 2019</p> <p>Storrs, CT, USA</p> <p>Spring 2019</p> <p>Spring 2017</p> <p>Spring 2017</p> <p>Spring 2016, Fall 2016</p>
STUDENTS	<p>New York University</p> <p>Master Students:</p> <ul style="list-style-type: none"> • 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 	<p>Brooklyn, NY, USA</p>

COMPETITION EXPERIENCES	<p>MITRE Embedded System CTF 2017 (First Place Overall, Iron Flag Award)</p> <p>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.</p> <ul style="list-style-type: none"> • 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.
PROFESSIONAL SERVICES	<p>Program Co-Chair & Co-Founder</p> <ul style="list-style-type: none"> • Int. Workshop on Critical Infrastructure and Manufacturing System Security (CIMSS'21) <p>Program Committee Member</p> <ul style="list-style-type: none"> • IFIP International Internet of Things Conference (IFIP IoT'21) • International Workshop on Security and Trust Management (STM'21) • Int. Conference on Information and Communications Security (ICICS'19, 20, 21) • Euromicro Conference on Digital Systems Design (DSD'21) • International Symposium on Quality Electronic Design (ISQED'20, 21) • Applied Research Competition in North American Region (CSAW'20) • Workshop on Attacks and Solutions in Hardware Security (ASHES'20) • International Conference on Science of Cyber Security (SciSec'19) <p>Student Program Committee Member</p> <ul style="list-style-type: none"> • IEEE Symposium on Security and Privacy (S&P'16) <p>Reviewer</p> <p><i>Journals</i></p> <ul style="list-style-type: none"> • 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 Electronic Testing (JETTA) • Springer Journal of Hardware and Systems Security (HASS) • Springer Cybersecurity • IET Circuits, Devices & Systems • MDPI Cryptography • MDPI Electronics • MDPI Sensors • MDPI Applied Sciences • Journal of Internet Technology (JIT) <p><i>Conferences</i></p> <ul style="list-style-type: none"> • 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) <p>Sub-Reviewer</p> <p><i>Journals</i></p> <ul style="list-style-type: none"> • 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)

TALKS

1. PwoP: Intrusion-Tolerant and Privacy-Preserving Sensor Fusion. *The Amsterdam Coordination Group (ACG) Meeting*. Virtual, 2021/3.
2. Securing Critical Infrastructures in Smart Cities. *TU Delft ENS Seminar*. Virtual, 2021/3.
3. Lightweight Signature Schemes for Cyber-Physical Systems. *The Conference for Information and Communications Technology Research in the Netherlands (ICT.OPEN)*. Virtual, 2021/2.
4. Erasable PUFs: Formal Treatment and Generic Design. *The Amsterdam Coordination Group (ACG) Meeting*. Virtual, 2020/12.
5. Erasable PUFs: Formal Treatment and Generic Design. *Workshop on Attacks and Solutions in Hardware Security (ASHES)*. Virtual, 2020/11.
6. Enhancing Cyber-Physical Systems Security with Cryptography and Hardware Security Primitives. *ECE Department Seminar*. Iowa State University, Ames, IA, USA, 2020/2.
7. Securing the Infrastructures in Smart Cities with Cryptography and Hardware Primitives. *Seminar*. Virginia Commonwealth University, Richmond, VA, USA, 2020/2.
8. Securing the Infrastructures in Smart Cities using Cryptography and Hardware Primitives. *Research Seminar*. Villanova University, Villanova, PA, USA, 2020/2.
9. Securing the Infrastructures in Smart Cities. *Center for Urban Science and Progress (CUSP) Research Seminar*. New York University, Brooklyn, NY, USA, 2019/9.
10. 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.
11. Enhancing Cyber-Physical System Security with Cryptography and Hardware Security Primitives. *Seminar*. Tennessee State University, Nashville, TN, USA, 2019/3.
12. Efficient Erasable PUFs from Programmable Logic and Memristors. *Connecticut Microelectronics and Optoelectronics Consortium Symposium*. University of New Haven, Orange, CT, USA, 2019/3.
13. Enhancing Cyber-Physical System Security with Cryptography and Hardware Security Primitives. *Seminar*. California State University, Long Beach, CA, USA, 2019/3.

14. Enhancing Cyber-Physical System Security with Cryptographic Primitives. *Seminar*. DePaul University, Chicago, IL, USA, 2019/2.
15. Enhancing Cyber-Physical System Security with Cryptography and Hardware Security Primitives. *Graduate Seminar*. University of Utah, Salt Lake City, UT, USA, 2019/2.
16. Cryptographic Solutions for Cyber-Physical System Security. *Seminar*. United Technologies Research Center, East Hartford, CT, USA, 2018/9.
17. PwoP: Intrusion-Tolerant and Privacy-Preserving Sensor Fusion. *Security Seminar*. University of Connecticut, Storrs, CT, USA, 2018/9.
18. Secure Sensor Fusion. *Modular Approach to Cloud Security (MACS) Project Meeting*. Boston University, Boston, MA, USA, 2018/1.
19. Advancing the State-of-the-Art in Hardware Trojans Design. *IEEE International Midwest Symposium on Circuits and Systems (MWSCAS)*. Medford, MA, USA, 2017/8.
20. 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.
21. Secure and Efficient Initialization and Authentication Protocols for SHIELD. *Security Seminar*. University of Connecticut, Storrs, CT, USA, 2016/9.
22. NREPO: Normal Basis Recomputing with Permuted Operands. *IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*. Washington, DC, USA, 2014/5.