

CONTACT INFORMATION	Science Park 123, 1098 XG Amsterdam, the Netherlands	Email: <a href="mailto:chenglu.jin@cw.nl">chenglu.jin@cw.nl</a> Website: <a href="https://chenglujin.github.io">chenglujin.github.io</a>
CURRENT POSITION	Researcher at <b>Centrum Wiskunde &amp; Informatica (CWI Amsterdam)</b> , the national research institute for mathematics and computer science in the Netherlands	
EDUCATION	<b>University of Connecticut</b>	Storrs, CT, USA
	Ph.D., Electrical Engineering, GPA: 4.08/4.0	Aug'19
	<ul style="list-style-type: none"> <li>Dissertation: <i>Cryptographic Solutions for Cyber-Physical System Security</i></li> <li>Advisor: Prof. Marten van Dijk</li> </ul>	
	<b>New York University</b>	Brooklyn, NY, USA
	M.S., Computer Engineering, GPA: 3.91/4.0	May'14
	<ul style="list-style-type: none"> <li>Thesis: <i>NREPO: Normal Basis Recomputing with Permuted Operands</i></li> <li>Advisor: Prof. Ramesh Karri</li> </ul>	
	<b>Xidian University</b>	Xi'an, China
	B.S., Electronic Information Science and Technology, GPA: 85/100	Jun'12
WORK AND RESEARCH EXPERIENCES	<b>Centrum Wiskunde &amp; Informatica</b>	Amsterdam, the Netherlands
	Tenured Researcher in the Computer Security Group	Sep'24 to Present
	<b>Centrum Wiskunde &amp; Informatica</b>	Amsterdam, the Netherlands
	Tenure-track Researcher in the Computer Security Group	Oct'20 to Sep'24
	<b>New York University</b>	Brooklyn, NY, USA
	Research Assistant Professor at CUSP and CCS	Mar'20 to Aug'20
	<b>New York University</b>	Brooklyn, NY, USA
	Smart Cities Postdoctoral Associate at CUSP and CCS	Sep'19 to Feb'20
	Advisers: Prof. Ramesh Karri and Prof. Daniel Neill	
	<b>University of Connecticut</b>	Storrs, CT, USA
	Research Assistant in the ECE Department	Aug'14 to Aug'19
	Adviser: Prof. Marten van Dijk	
	<b>Singapore University of Technology and Design</b>	Singapore
	Intern at iTrust	May'18 to Aug'18
	Mentor: Prof. Jianying Zhou	
	<b>Open Security Research</b>	Shenzhen, China
	Intern	Jun'16 to Aug'16
	Mentor: Dr. Junfeng Fan	
	<b>Open Security Research</b>	Shenzhen, China
	Intern	Jun'15 to Aug'15
	Mentor: Dr. Junfeng Fan	
	<b>New York University</b>	Brooklyn, NY, USA
	Research Assistant	Sep'13 to May'14
	Adviser: Prof. Ramesh Karri	

## FUNDING

**Centrum Wiskunde & Informatica**, Amsterdam, the Netherlands

- **NWO** Gravitation: Challenges in Cyber Security (Phase I awarded: €9.93M. Role: **Team Member**.)

**New York University**, Brooklyn, NY, USA

- **US ARMY** STTR: Fully-digital mmWave Lens-Antenna System for Resilient Tactical Communications (Phase I awarded: \$166K. Role: **Co-PI**.)

## Publications

\* denotes shared first authorship. † denotes alphabetical authorship.

### 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. X. Cao, Z. Yang, J. Ning, **C. Jin**, R. Lu, Z. Liu, and J. Zhou. (2024) “Dynamic Group Time-based One-time Passwords.” In *IEEE Transactions on Information Forensics and Security (TIFS)*.
3. Q. Liu, Y. Huang, **C. Jin**, X. Zhou, Y. Mao, C. Catal, and L. Cheng. (2024) “Privacy and Integrity Protection for IoT Multimodal Data using Machine Learning and Blockchain.” In *ACM Transactions on Multimedia Computing Communications and Applications (TOMM)*.
4. Z. Yang\*, **C. Jin\***, X. Cao, M. van Dijk, and J. Zhou. (2023) “Optimizing Proof of Aliveness in Cyber-Physical Systems.” In *IEEE Transactions on Dependable and Secure Computing (TDSC)*.
5. D. Gurevin, **C. Jin**, P. H. Nguyen, O. Khan, and M. van Dijk. (2023) “Secure Remote Attestation with Strong Key Insulation Guarantees.” In *IEEE Transactions on Computers (TC)*.
6. M. van Dijk and **C. Jin**. (2023) “A Theoretical Framework for the Analysis of Physical Unclonable Function Interfaces and its Relation to the Random Oracle Model.” In *Journal of Cryptology (JoC)*.
7. **C. Jin\***, Z. Yang\*, T. Xiang, S. Adepur, and J. Zhou. (2023) “HMACCE: Establishing Authenticated and Confidential Channel from Historical Data for Industrial Internet of Things.” In *IEEE Transactions on Information Forensics and Security (TIFS)*.
8. **C. Jin**, W. Burleson, M. van Dijk, and U. Rührmair. (2022) “Programmable Access-Controlled and Generic Erasable PUF Design and Its Applications.” In *Journal of Cryptographic Engineering (JCEN)*.
9. Z. Yang, Z. Bao, **C. Jin**, Z. Liu, and J. Zhou. (2021) “PLCrypto: A Symmetric Cryptographic Library for Programmable Logic Controllers.” In *IACR Transactions on Symmetric Cryptology (ToSC, formerly known as Fast Software Encryption conference (FSE))*. (Acceptance rate of Issue 3:  $7/44 = 15.9\%$ )
10. 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*.
11. 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)*.

12. 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:  $42/214 = 19.7\%$ )
13. **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)*.
14. 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**
  - **Featured in “Spotlight on Transactions” in IEEE Computer, June 2019**
15. **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**
16. 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)*.
17. 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

18. S. Shen, and **C. Jin**. (2024) “Reading It Like an Open Book: Single-trace Blind Side-channel Attacks on Garbled Circuit Frameworks.” In *2024 Annual Computer Security Applications Conference (ACSAC)*.
  - **Artifacts Evaluated Reusable; Results Reproducible**
19. **C. Jin\***, C. Yin\*, M. van Dijk, S. Duan, F. Massacci, M. K. Reiter, and H. Zhang (2024, Oct) “PG: Byzantine Fault-Tolerant and Privacy-Preserving Sensor Fusion with Guaranteed Output Delivery.” In *2024 ACM Conference on Computer and Communications Security (CCS)*.
  - **Artifacts Evaluated Functional**
20. Z. DiMeglio, J. Bustami, D. Gurevin, **C. Jin**, M. van Dijk, and O. Khan. (2024, May) “Masked Memory Primitive for Key Insulated Schemes.” In *2024 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*. (Acceptance rate:  $32/139 = 23.0\%$ )
21. Z. Yang, **C. Jin**, J. Ning, Z. Li, T. T. A. Dihn, and J. Zhou. (2021, Dec) “Group Time-based One-time Passwords and its Application to Efficient Privacy-Preserving Proof of Location.” In *2021 Annual Computer Security Applications Conference (ACSAC)*. (Acceptance rate:  $80/326 = 24.5\%$ )
22. Z. Yang, **C. Jin**, Y. Tian, J. Lai, and 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:  $67/308 = 21.8\%$ )

23. **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 Functional**

24. 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**

25. **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)*.
26. M. van Dijk<sup>†</sup>, **C. Jin**<sup>†</sup>, H. Maleki<sup>†</sup>, P. H. Nguyen<sup>†</sup>, and R. Rahaeimehr<sup>†</sup>. (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:  $27/110 = 24.5\%$ )
27. 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:  $49/208 = 23.6\%$ )
28. 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)*.
29. 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:  $18/106 = 17.0\%$ )
30. 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:  $17/71 = 23.9\%$ )
31. 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

32. 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)*.
33. **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)*.

	34. <b>C. Jin</b> , L. Ren, X. Liu, P. Zhang, and M. van Dijk. (2017, Apr) “Mitigating Synchronized Hardware Trojan Attacks in Smart Grids.” In <i>2017 Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG@CPSWeek)</i> .
PRE-PRINTS	35. N. Sayadi, P. H. Nguyen, M. van Dijk, and <b>C. Jin</b> . (2023) “Breaking XOR Arbiter PUFs without Reliability Information.” <i>arXiv</i> .
	36. M. van Dijk <sup>†</sup> , D. Gurevin <sup>†</sup> , <b>C. Jin</b> <sup>†</sup> , O. Khan <sup>†</sup> , and P. H. Nguyen <sup>†</sup> . (2021) “Autonomous Secure Remote Attestation even when all Used and to be Used Digital Keys Leak.” <i>Cryptography ePrint Archive</i> .
	37. <b>C. Jin</b> , V. Gohil, R. Karri, and J. Rajendran. (2020) “Security of Cloud FPGAs: A Survey.” <i>arXiv</i> .
AWARDS	<ul style="list-style-type: none"> <li>• Best Paper Award Candidate IEEE-NANO 2019</li> <li>• First Place Overall MITRE eCTF 2017</li> <li>• Iron Flag Award MITRE eCTF 2017</li> <li>• Doctoral Dissertation Fellowship UConn Graduate School 2019</li> <li>• Predoctoral Summer Research Fellowship UConn ECE Dept. 2017</li> <li>• Student Travel Award CHES 2019</li> <li>• Student Scholarship BlackHat USA 2017</li> <li>• Student Travel Award HOST 2017</li> <li>• Student Travel Award Real World Crypto 2016</li> </ul>
TEACHING EXPERIENCES	<p><b>University of Amsterdam</b> Amsterdam, the Netherlands</p> <p><b>Mentor:</b></p> <ul style="list-style-type: none"> <li>• <i>Research Project in Security and Network Engineering</i> Spring 2024</li> </ul> <p><b>Guest Lecturer (on Anonymity &amp; Privacy):</b></p> <ul style="list-style-type: none"> <li>• <i>Introduction to Security</i> Sep 2024</li> </ul> <p><b>Guest Lecturer (on Physical Unclonable Functions):</b></p> <ul style="list-style-type: none"> <li>• <i>Cryptographic Engineering</i> Mar 2023, Mar 2024</li> </ul> <p><b>King Abdullah University of Science and Technology</b> Thuwal, Saudi Arabia</p> <p><b>Guest Lecturer (on Hardware Security):</b></p> <ul style="list-style-type: none"> <li>• <i>Computer Systems Security</i> Apr 2022, Nov 2022, Nov 2023, Nov 2024</li> </ul> <p><b>New York University</b> Brooklyn, NY, USA</p> <p><b>Course Co-developer:</b></p> <ul style="list-style-type: none"> <li>• <i>Cybersecurity in Additive Manufacturing</i> Fall 2020</li> </ul> <p><b>Master Capstone Project Mentor:</b></p> <ul style="list-style-type: none"> <li>• <i>Urban Science Intensive</i> Spring 2020, Summer 2020</li> </ul> <p><b>Teaching Assistant:</b></p> <ul style="list-style-type: none"> <li>• <i>Introduction to Hardware Security and Trust</i> Spring 2020</li> <li>• <i>Advanced Computer Hardware Design</i> Fall 2019</li> </ul> <p><b>University of Connecticut</b> Storrs, CT, USA</p> <p><b>Instructor and Course Developer:</b></p> <ul style="list-style-type: none"> <li>• <i>Seminar on Cyber-Physical System Security</i> Spring 2019</li> </ul> <p><b>Course Co-developer:</b></p> <ul style="list-style-type: none"> <li>• <i>Advanced Microprocessor Application Lab</i> Spring 2017</li> <li>• <i>Introduction to Hardware Security and Trust</i> Spring 2017</li> </ul> <p><b>Teaching Assistant:</b></p> <ul style="list-style-type: none"> <li>• <i>Microprocessor Applications Laboratory</i> Spring 2016, Fall 2016</li> </ul>

STUDENTS	<b>Centrum Wiskunde &amp; Informatica</b>	Amsterdam, the Netherlands
	<b>Ph.D. Students:</b>	
	<ul style="list-style-type: none"> <li>• Niloufar Sayadi, 2023 - present (Co-advised with Prof. Marten van Dijk)</li> <li>• Sirui Shen, 2023 - present (Co-advised with Prof. Marten van Dijk)</li> </ul>	
	<b>University of Amsterdam</b>	Amsterdam, the Netherlands
	<b>Master Students:</b>	
	<ul style="list-style-type: none"> <li>• Isaac Santhagens, 2024</li> <li>• James Karsten, 2024</li> <li>• Roberto Volpe Garcia, 2024</li> <li>• Jan Laan and Wendy Roks, 2024</li> </ul>	
	<b>Wageningen University &amp; Research</b>	Wageningen, the Netherlands
	<b>Master Students:</b>	
	<ul style="list-style-type: none"> <li>• Yuchen Huang, 2022 (Co-advised with Dr. Qingzhi Liu)</li> </ul>	
	<b>New York University</b>	Brooklyn, NY, USA
	<b>Master Students:</b>	
	<ul style="list-style-type: none"> <li>• Shreeraman Arunachalam Karikalan, Aparna Bhutani, Siqi Huang, and Vivek Patel, 2020</li> <li>• Guilherme Louzada, Chenjie Su, Akash Yadav, Eric Zhuang, 2020</li> </ul>	
COMPETITION EXPERIENCES	<b>MITRE Embedded System CTF 2017 (First Place Overall, Iron Flag Award)</b>	
	<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"> <li>• Won <b>First Place Overall</b> counting all the points gained by attacks and defenses.</li> <li>• Won <b>Iron Flag Award</b> for successfully designing a secure system that defended every flag from its attackers in the whole competition.</li> </ul>	
PROFESSIONAL SERVICES	<b>Co-Leader</b>	
	<ul style="list-style-type: none"> <li>• Hardware and Cyber-Physical System Security Working Group in ACademic Cyber Security Society in the Netherlands (ACCSS)</li> </ul>	
	<b>Guest Editor</b>	
	<ul style="list-style-type: none"> <li>• Wireless Communications and Mobile Computing (WCMC), Special Issue on “Intelligent and Flexible Security of Next-Generation Wireless Networks ”</li> </ul>	
	<b>Funding Proposal Reviewer</b>	
	<ul style="list-style-type: none"> <li>• Luxembourg National Research Fund (FNR)</li> </ul>	
	<b>Program Committee Co-Chair &amp; Co-Founder</b>	
	<ul style="list-style-type: none"> <li>• International Workshop on Critical Infrastructure and Manufacturing System Security (CIMSS’21, 22)</li> </ul>	
	<b>Program Committee Member</b>	
	<ul style="list-style-type: none"> <li>• International Conference on Financial Cryptography and Data Security (FC’25)</li> <li>• International Symposium on Quality Electronic Design (ISQED’20 - 25)</li> <li>• ACM Asia Conference on Computer and Communications Security (AsiaCCS’25)</li> <li>• IACR Conference on Cryptographic Hardware and Embedded Systems (CHES’25)</li> <li>• ACM Cloud Computing Security Workshop (CCSW’21 - 24)</li> <li>• Workshop on Attacks and Solutions in Hardware Security (ASHES’20 - 24)</li> <li>• International Workshop on Security and Trust Management (STM’21 - 24)</li> <li>• IEEE Conference on Communications and Network Security (CNS’22 - 24)</li> <li>• IEEE International Conference on Omni-Layer Intelligent Systems (COINS’23, 24)</li> <li>• Malicious Software and Hardware in Internet of Things (MaL-IoT’23, 24)</li> <li>• IEEE International Conference on Cyber, Physical and Social Computing (CPSCoM’24)</li> </ul>	

- ACM Cyber-Physical System Security Workshop (CPSS'24)
- Applied Research Competition in North American Region (CSAW'20, 23)
- IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom'23)
- IFIP International Internet of Things Conference (IFIP IoT'21, 22)
- International Conference on Information and Communications Security (ICICS'19 - 22)
- Euromicro Conference on Digital Systems Design (DSD'21)
- 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 Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)
- IEEE Transactions on Very Large Scale Integration Systems (TVLSI)
- IEEE Transactions on Circuits and Systems I (TCAS-I)
- IEEE Transactions on Industrial Informatics (TII)
- IEEE Transactions on Reliability (TR)
- IEEE Transactions on Consumer Electronics (TCE)
- IEEE Security & Privacy (SP)
- IEEE Computer Architecture Letters (CAL)
- IEEE Internet of Things Journal (IOT-J)
- IEEE Consumer Electronics Magazine (CEM)
- IEEE Access
- ACM Computing Surveys (CSUR)
- ACM Transactions on Privacy and Security (TOPS)
- ACM Transactions on Reconfigurable Technology and Systems (TRETs)
- ACM Transactions on Design Automation of Electronic Systems (TODAES)
- ACM Transactions on Embedded Computing Systems (TECS)
- ACM Journal on Emerging Technologies in Computing Systems (JETC)
- IOS Journal of Computer Security (JCS)
- Springer Journal of Cryptographic Engineering (JCEN)
- Springer Journal of Electronic Testing (JETTA)
- Springer Journal of Hardware and Systems Security (HASS)
- Springer International Journal of Information Security (IJIS)
- Springer Cybersecurity
- Springer Discover Internet of Things
- IET Circuits, Devices & Systems
- MDPI Cryptography
- MDPI Electronics
- MDPI Sensors
- MDPI Applied Sciences
- Journal of Internet Technology (JIT)

##### *Conferences*

- ACM/EDAC/IEEE Design Automation Conference (DAC'18 - 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 Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)

#### *Conferences*

- Design, Automation and Test in Europe Conference (DATE'22)
- International Test Conference (ITC'20)
- ACM/EDAC/IEEE Design Automation Conference (DAC'15 - 17, 20)
- ACM conference on Computer and Communications Security (CCS'17, 19)
- IEEE International Symposium on Hardware-Oriented Security and Trust (HOST'15 - 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)

#### **Publicity Chair**

- International Workshop on Critical Infrastructure and Manufacturing System Security (CIMSS'23)
- EAI International Conference on Applied Cryptography in Computer and Communications (EAI AC3'22)

#### TALKS

1. PG: Byzantine Fault-Tolerant and Privacy-Preserving Sensor Fusion with Guaranteed Output Delivery. *Seminar at Radboud University*, Nijmegen, the Netherlands, 2024/6.
2. Recent Advances in the Attacks and Applications of Silicon PUFs. *Seminar at University of Twente*, Enschede, the Netherlands, 2024/6.
3. Towards Remote Verifiable Computation without Digital Secrets. *Seminar at Shandong University*, Virtual, 2023/11.
4. Towards Remote Verifiable Computation without Digital Secrets. *Crypto Working Group Meetup*, Utrecht, the Netherlands, 2023/9.
5. HMACCE: Establishing Authenticated and Confidential Channel from Historical Data for IIoT. *The Conference for Information and Communications Technology Research in the Netherlands (ICT.OPEN)*, Utrecht, the Netherlands, 2023/4.
6. HMACCE: Establishing Authenticated and Confidential Channel from Historical Data for Industrial Internet of Things. *Invited Talk at University of Strathclyde*, Virtual, 2023/2.
7. Attacking Physical Unclonable Functions Using Machine Learning. *Amsterdam Data Science Meetup*, Amsterdam, the Netherlands, 2022/12.
8. PwoP: Intrusion-Tolerant and Privacy-Preserving Sensor Fusion. *CWI Scientific Meeting*, Amsterdam, the Netherlands, 2022/5.
9. Group Time-based One-time Passwords and its Application to Efficient Privacy-Preserving Proof of Location. *2021 Annual Computer Security Applications Conference (ACSAC)*, Virtual, 2021/12.
10. Securing Critical Infrastructures in Smart Cities. *Cryptographic Engineering Research Forum at Nanjing University of Aeronautics and Astronautics*, Virtual, 2021/8.



11. PwoP: Intrusion-Tolerant and Privacy-Preserving Sensor Fusion. *The Amsterdam Coordination Group (ACG) Meeting at CWI Amsterdam*, Virtual, 2021/3.
12. Securing Critical Infrastructures in Smart Cities. *ENS Seminar at Delft University of Technology*, Virtual, 2021/3.
13. Lightweight Signature Schemes for Cyber-Physical Systems. *The Conference for Information and Communications Technology Research in the Netherlands (ICT.OPEN)*, Virtual, 2021/2.
14. Erasable PUFs: Formal Treatment and Generic Design. *The Amsterdam Coordination Group (ACG) Meeting at CWI Amsterdam*, Virtual, 2020/12.
15. Erasable PUFs: Formal Treatment and Generic Design. *Workshop on Attacks and Solutions in Hardware Security (ASHES)*, Virtual, 2020/11.
16. Enhancing Cyber-Physical Systems Security with Cryptography and Hardware Security Primitives. *ECE Department Seminar at Iowa State University*, Ames, IA, USA, 2020/2.
17. Securing the Infrastructures in Smart Cities with Cryptography and Hardware Primitives. *Seminar at Virginia Commonwealth University*, Richmond, VA, USA, 2020/2.
18. Securing the Infrastructures in Smart Cities using Cryptography and Hardware Primitives. *Research Seminar at Villanova University*, Villanova, PA, USA, 2020/2.
19. Securing the Infrastructures in Smart Cities. *Center for Urban Science and Progress (CUSP) Research Seminar at New York University*, Brooklyn, NY, USA, 2019/9.
20. 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.
21. Enhancing Cyber-Physical System Security with Cryptography and Hardware Security Primitives. *Seminar at Tennessee State University*, Nashville, TN, USA, 2019/3.
22. Efficient Erasable PUFs from Programmable Logic and Memristors. *Connecticut Microelectronics and Optoelectronics Consortium Symposium at University of New Haven*, Orange, CT, USA, 2019/3.
23. Enhancing Cyber-Physical System Security with Cryptography and Hardware Security Primitives. *Seminar at California State University*, Long Beach, CA, USA, 2019/3.
24. Enhancing Cyber-Physical System Security with Cryptographic Primitives. *Seminar at DePaul University*, Chicago, IL, USA, 2019/2.
25. Enhancing Cyber-Physical System Security with Cryptography and Hardware Security Primitives. *Graduate Seminar at University of Utah*, Salt Lake City, UT, USA, 2019/2.
26. Cryptographic Solutions for Cyber-Physical System Security. *Seminar at United Technologies Research Center*, East Hartford, CT, USA, 2018/9.
27. PwoP: Intrusion-Tolerant and Privacy-Preserving Sensor Fusion. *Security Seminar at University of Connecticut*, Storrs, CT, USA, 2018/9.

28. Secure Sensor Fusion. *Modular Approach to Cloud Security (MACS) Project Meeting at Boston University*, Boston, MA, USA, 2018/1.
29. Advancing the State-of-the-Art in Hardware Trojans Design. *IEEE International Midwest Symposium on Circuits and Systems (MWSCAS)*, Medford, MA, USA, 2017/8.
30. 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.
31. Secure and Efficient Initialization and Authentication Protocols for SHIELD. *Security Seminar at University of Connecticut*, Storrs, CT, USA, 2016/9.
32. NREPO: Normal Basis Recomputing with Permuted Operands. *IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, Washington, DC, USA, 2014/5.